GAZİ ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ - BİLGİSAYAR MÜHENDİSLİĞİ

171180010 – Cansu AYTEN

BM402 BİLGİSAYAR AĞLARI

ÖDEV 3: Protokol saldırıları ve önlemleri

Mart 2022

İÇİNDEKİLER

Sayfa

İÇİNDEKİLER i
1. PROTOKOL SALDIRILARI 1
1.1 DNS 1
1.1.2 DNS Saldırıları Önlemleri 2
1.2 TCP 2
1.2.1 TCP Saldırıları 2
1.2.2 TCP Saldırıları Önlemleri 3
1.3 IP 3
1.3.1 IP Saldırıları 4
1.3.2 IP Saldırıları Önlemleri 4
1.4 FTP 4
1.4.1 FTP Saldırıları 4
1.4.2 FTP Saldırıları Önlemleri 5
1.5 ICMP 5
1.5.1 ICMP Saldırıları 5
1.5.2 ICMP Saldırıları Önlemleri 6
1.6 UDP 6
1.6.1 UDP Saldırıları 6
1.6.2 UDP Saldırıları Önlemleri 6
1.7 ARP 6
1.7.1 ARP Saldırıları 7
1.7.2 ARP Saldırıları Önlemleri 7
KAYNAKÇA 8

1. PROTOKOL SALDIRILARI

1.1 DNS

Bilgisayarların birbiriyle iletişimi için kullanılan IP adreslerini hatırlamak, okumak ya da akılda tutmak zordur. Bu nedenle insanlar tarafından okunması ve akılda tutması daha kolay olan alan adları kullanılmaktadır. Bilgisayarların alan adları yardımıyla haberleşmesi için ortaya çıkan Domain Name System'in (alan isimlendirme sistemi) kısaltması olan DNS, isimleri IP adreslerine çevirmek için kullanılan bir sistemdir. Bir telefon rehberi gibi çalışır. Örneğin telefonda aramak istediğimiz kişiyi ararken ismini bulup numarası ile ararız. DNS'de benzer mantıkla çalışmaktadır. Tarayıcıda girilmek istenilen web sitesinin alan adı yazılır. Daha sonrasında DNS ile o alan adına ait IP adresi bulunup istek gönderilir. DNS uygulama katmanında bulunmaktadır [1].

1.1.1 DNS Saldırıları

DNS saldırıları DNS'deki güvenlik açıkları nedeniyle meydana gelen saldırılardır. Bu saldırılarda istemci ile sunucu arasındaki iletişimden yararlanılır. Sıfır gün saldırısı, Önbellek zehirlenmesi, DOS, DDoS DNS, TCP Reset, TCP Session Hijacking, saldırı türleridir.

- **Sıfır Gün Saldırısı:** Bir DNS protokolünde bir güvenlik açığının geliştiricilerden önce kötü niyetli kişiler tarafından tespit edilmesiyle meydana gelir. Bu güvenlik açığının bulunduğu gün saldırı gerçekleştiği için adı sıfır gün saldırısıdır [3].
- **DNS Önbellek Zehirlenmesi (DNS spoofing):** Kullanılan DNS sunucuları daha önceki sorgular sayesinde önbelleğe alınır. Önbellekteki verilerin değişmesi ya da yanlış bilgi girilmesi nedeniyle yanlış yanıt gelmesi veya yanlış web sitelerine yönlendirilmesine DNS önbellek zehirlenmesi denir. Yönlendirilen hatalı site kötü amaçlı bir site olabilir. Böylelikle kullanıcı risk altında kalır. Hatalı bir DNS bilgisinin yaşam süresi (TTL) sona erene kadar veya manuel olarak kaldırılana kadar önbellekte kalacaktır [2].
- **Denial of Service (DoS):** DoS saldırılarıyla sistemler hizmet veremez duruma gelirler. Yapılması ve önlenmesi kolay bir saldırı türüdür. Bir saldırgan ya da bot ile bir IP adresine çok fazla trafik oluşturulmasıyla ya da çok fazla istek gönderilmesiyle birlikte sunucunun yanıt veremez hale gelmesidir.
- **Distributed Denial of Service (DDoS):** Tek bir saldırgan tarafından oluşturulan farklı IP'lerin trafik oluşturması ve fazla istek göndermesiyle sunucunun hizmet veremez hale gelmesine denir. Kısaca DoS saldırılarının dağıtık yapılmasıdır. Engellenmesi zordur

- **DNS Amplification:** DDoS türlerinden biridir. Amaç DDoS'takiyle aynı olup sistemleri yavaşlatıp hizmet veremez duruma getirmektir. Bu gerçekleştirilirken ağ bant genişliği sistem çalıştırılamaz hale gelinceye kadar sahte DNS istekleri doldurulur. Bu tür saldırılar hacimsel saldırılardır.
- **Fast-flux DNS:** Kötü niyetli kişiler ya da saldırganların birden çok IP adresini tek bir alanla ilişkilendirmesi ve bu IP adreslerini sürekli değiştirmesi yöntemine Fast-flux DNS denmektedir. Saldırganın amacı yapılacak kötü işlemlerin gerçek kaynağını gizlemek ve güvenlik ekiplerinin bu işlemlerin kaynağını engellemesini önlemektir [4].

1.1.2 DNS Saldırıları Önlemleri

DNS'e yapılan saldırıları önlemek için ya da saldırı olma olasılığını azaltmak için alınabilecek bazı önlemler mevcuttur. Bunlardan biri DNS yazılımının güncel sürümünü kullanmaktır. Diğeri trafiğin sürekli izlenmesidir. Sorguların ve yanıtların günlüğe kaydedilip anormalliklerin tespit edilmesi gereklidir. Bir diğeri ise sunucuları istenmeyen erişimlere karşı korumaktır. Şirketlerde DNS saldırılarına karşı önlem almak amacıyla çok faktörlü kimlik doğrulama etkinleştirilebilir [3,5].

1.2 TCP

Transmission Control Protocol'ün kısaltılmışı olan TCP protokolü paket anahtarlamalı ağlarda paketin mutlaka ulaştırılacağını, ulaştırılamasa bile ulaştırılana kadar tekrar deneneceğini garantileyen amacı paket kayıplarını engellemek olan bir protokoldür. Bu protokol yalnızca paketleri ulaştırmakla kısıtlı kalmaz, ulaşan paketleri doğru bir şekilde sıraya da sokar. İletişim kanalına güvenilirlik ekler. TCP ulaşım katmanında bulunmaktadır.

1.2.1 TCP Saldırıları

- **SYN Flooding Saldırısı:** Popüler bir DoS saldırısı türüdür. TCP protokolü ile istemci bir sunucuyla bağlantı kurmak istediğinde TCP üç yollu el sıkışma (TCP Three Way Handshake) işlemi meydana gelir. Bu işlem üç adımdan meydana gelir. İlk adımda istemci sunucuya SYN paketi gönderir. İkinci adımda sunucu istemcinin gönderdiği paketi alıp istemciye paketi aldığına dair bir SYN-ACK paketi gönderir. En son istemci sunucunun gönderdiği paketi aldığını belirtmek için sunucuya ACK mesajını gönderir. Bu saldırıda sunucunun hizmet verememesi için çok sayıda SYN isteğinin art arda ve hızlı bir şekilde gönderilmesiyle birlikte paketler için ayrılan alanın dolması sonucu sunucu çalışamaz hale gelmektedir [6,7].

- **TCP Reset Saldırısı:** Bir saldırgan tarafından iki kurban arası iletişimin sahte bir TCP paketiyle kesilmesidir [8]. Kötü niyetli kişiler tarafından sahte TCP sıfırlama paketleriyle İnternet bağlantısı kurcalanabilir veya sonlandırılabilir [9].
- **TCP Session Hijacking Saldırısı:** Kötü niyetli kişinin bir kurbanın oturumuna erişmesiyle o kullanıcı gibi davranarak kullanıcının yetkisinde olan bütün işlemleri yerine getirmesidir. Kurbanın oturumuna erişmesiyle birlikte bu oturum etkin olduğu süre boyunca kurbanın yetkisi dâhilindeki işlemlerde herhangi bir kimlik doğrulaması yapmasına gerek kalmaz. Çünkü kullanıcı saldırıdan önce zaten kimlik doğrulaması yapmıştır [10].

1.2.2 TCP Saldırıları Önlemleri

- **SYN Flooding Saldırılarını Azaltmak için Yapılabilecekler:**
  Sunucunun bağlantı isteği kapasitesini yani belleği artırmak fazla istek gelse bile sunucu performansının olumsuz etkilenmemesini sağlayabilir. Bir diğeri ise istemcinin sunucuya SYN paketini göndermesinin ardından sunucu da istemciye SYN-ACK paketini göndermiş ve artık sunucu istemciden ACK paketini bekliyorsa bu kurulan bağlantıların en eskiden yeniye doğru sıralanarak en eski bağlantıları yok etmek belleği rahatlatmak için bir çözüm olabilir. Bir diğer çözüm ise ACK paketlerinin dönüşü için kullanılan timer'da belirlenen süreyi kısaltmaktır. Böylelikle bu süre içerisinde gelmeyen ACK paketlerine ait bağlantılara son verilir ve bellek rahatlar [11].
- **TCP Session Hijacking Saldırısı için Önlemler:**
  TCP Session Hijacking Saldırısı için alınabilecek önlemlerden biri şifrelemedir. Güvenli bir iletim ortamı sağlamak amacıyla SSH protokolü kullanılabilir. Bir diğer önlem ise IDS ve IPS sistemleridir. Bu sistemler anormal veya zararlı hareketleri tespit edip kaydederek önlenmesini sağlarlar. Bir diğer önlem ise VPN kullanmak olabilir. Başka bir önlem ise her hesap için aynı kullanıcı adı veya şifre kullanmak yerine farklı kullanıcı adı ve şifreler kullanılarak riski azaltmaktır. Herhangi biri saldırgan tarafından kullanıcı adı veya şifre tespit edilirse bununla aynı kullanıcı adı ya da şifreyi taşıyan diğer hesaplar da tehlikeye girer [10,12].

1.3 IP

İnternet Protokolü'nün kısaltılmışı olan IP protokolü, cihazın bir ağdaki diğer cihazlarla iletişim kurmasına olanak tanıyan kurallardır. Bu protokol paketlerin doğru adrese varmasını sağlamaktır. Bu durum verileri daha küçük parçalar olan paketlere bölünmesinin ardından pakete eklenen IP bilgisiyle başarılır. İnternete bağlı cihazlara atanan IP adresine göre bu

paketler uygun adreslere gönderilir. Bu protokol “best effort” yani elinden gelenin en iyisini yapacağını belirten ancak hedefe ulaştırma garantisi vermeyen bir protokoldür. Protokol ağda tıkanıklık varsa ulaştıramayabilir, problem yoksa ulaştırabilir. Kesinlik yoktur. İletimde “bu sürede veya bu hızda” şeklinde bir garanti de vermez. Paketler ağ üzerinde farklı yollar üzerinden hedefe ulaşabileceğinden gecikmeler yaşanabilir. Bu protokol ağ katmanında yer almaktadır.

1.3.1 IP Saldırıları

- **IP Spoofing:** Sahte kaynak adresine sahip sahte paketlerin oluşturulduğu bir işlemdir. Bu işlemin amacı göndericinin kimliğini gizlemek, başka bir kimliğe bürünmek veya her ikisi birden olabilir. Kısaca amaç saldırılarda tespit edilmekten kaçınmaya çalışmaktır. Saldırganlar DDoS saldırılarını ya da DoS saldırılarını bu yöntem ile gerçekleştirebilir [13].

1.3.2 IP Saldırıları Önlemleri

- **IP Spoofing için Önlemler:**
  IP Spoofing tam olarak önlenemez. Sadece birkaç yöntem ile savunma yapılabilir. Bunlardan biri giriş filtrelemedir. Gelen paketler ve kaynak başlıkları incelenir. Bir şüpheli durum tespit edilirse paketler reddedilir. Giden paketler de filtreleme yapılabilir. Bu işlemde ise giden paketlerin meşru kaynak başlıkları olup olmaması incelenir. Yalnızca meşru olanların çıkacağı bir filtreleme işlemi uygulanır. Böylelikle bir saldırının başlaması engellenebilir [13].

1.4 FTP

File Transfer Protocol’ün kısaltılmışı olan FTP protokolü İnternete bağlı iki cihaz arası dosya aktarımının gerçekleşmesinde kullanılan kurallardır. FTP eski bir protokoldür dolayısıyla günümüz ölçütlerinde çok sayıda güvenlik açığına sahiptir. Bu protokol uygulama katmanında yer almaktadır [14].

1.4.1 FTP Saldırıları

- **Anonim Kimlik Doğrulama:** Kullanıcılar bir kullanıcı adıyla ya da anonim olarak oturum açabilirler. Anonim olarak oturum açarken kullanıcılar kullanıcı adı olarak anonymous şifre olarak ise bir e-posta adresi girerler. Fakat kullanıcı adı, şifre ve kullanılan komutlar gibi verilerin şifrelenmemiş olması kolay ulaşılabilir olduğu anlamına gelmektedir. Buna ek olarak FTP kullanılarak aktarılan veriler de risk altındadır. Dolayısıyla bu bir güvenlik açığıdır [15].

- **Bounce Saldırısı:** FTP sunucusunun Proxy olarak kullanarak kötü niyetli kişinin iz bırakmadan saldırı yapabilmesidir. Genelde trafiği başka bir sunucuya yönlendirmek amacıyla gerçekleştirilir. Bu yöntemle birlikte bağlantı noktası taraması ve temel paket süzgeçlerinden geçmek yapılabilecek bazı saldırı türleri vardır [16].

1.4.2 FTP Saldırıları Önlemleri

FTP eski bir protokol olduğundan günümüz standartlarında çok fazla güvenlik açığına sahiptir. Gizlilik ve bütünlüğün bulunmamasının yanında saldırganların verilere ulaşması ve değiştirmesi de bu protokolde kolaydır. Bu nedenle yapılabileceklerden biri FTP'yi kullanmamaktır. Diğeri ise anonim kullanıcılara izin vermemektir. Kullanıcı adlarının karakter boyutunun en az yedi olması ve belli bir süre kullanılmayan hesapların ya da altı kez oturum açma hatası yaşanılan hesapların kapatılması gibi kurallar gereklidir. Bunlar dışındaki bir diğer önlem ise güçlü bir şifre belirlemektir. Kullanıcı adında olduğu gibi şifrelerin de karakter uzunluğu en az 7 olmalıdır. Şifrenin güçlü bir şifre olabilmesi için sayı, harf ve en az bir tane özel karakter içermesi gerekmektedir. Ayrıca şifreler belirli bir süre sonra değiştirilmesi ve değiştirilen şifrelerin son dört şifreden biri olmaması gerekmektedir [17].

1.5 ICMP

Internet Control Message Protocol'ün kısaltılmışı olan ICMP protokolü iletişim sorunlarını raporlamak amacıyla kullanılır. Bir sorun yaşanması halinde geri besleme mekanizması olduğundan TCP/IP'ye yardımcı olabilir. Çünkü IP hata bulma, bildirme, düzeltme becerilerden yoksundur. Bir sorun olması durumunda geri bildirimi sağlamak amacıyla her sunucuda ICMP protokolü çalışmaktadır. Bu protokol ağ katmanında yer almaktadır [18].

1.5.1 ICMP Saldırıları

- **Smurf Saldırısı:** Saldırgan hedefin sahte kaynak IP'sine birçok ICMP paketi gönderir. Ağdaki diğer cihazlar bu kaynak yanıt olarak paket gönderirler. O kadar çok paket gönderilir ki hedefin trafiği aşırı yoğunlaşır. Bunun sonucunda da hedef çalışamayacak duruma gelir ve hizmet veremez [19].
- **ICMP Flood Saldırısı:** Hedef cihaza sürekli büyük boyutlardaki PING paketleri gönderilir. Gelen paketler işlenip yanıtlanması gerekeceği için bir süre sonra kaynak yetmez ve hedef cihaz hizmet veremez hale gelir [18].
- **Ping of Death:** Hedef cihaza gönderilen IP paketi belirli boyutlar arasında olmalıdır. Bu boyutlar 216 bayt ile 65.536 bayttır. Saldırgan bu boyuttan daha büyük boyutta bir paket gönderirse bu paket hedef cihaza giderken parçalanır. Hedef cihaz bu parçaları

birleştirdiğinde boyutu aştığını görür. Bu durum cihazda arabellek taşması meydana getirir. Hedef cihaz çalışamaz duruma gelir. Bu durum eski cihazlarda yaşanabilir fakat yeni cihazlarda savunmalar mevcut olduğu için bu saldırılar artık bir sorun teşkil etmemektedir [18, 20].

1.5.2 ICMP Saldırıları Önlemleri

ICMP saldırılarını önlemek amacıyla ağa yönlendirilen trafik engellenmelidir. Başka bir önlem olarak oluşan hatalara kötü niyetli kişiler tarafından ulaşılamaması amacıyla hata mesajları dışarı çıkmamalıdır. Gelen ICMP paketleri boyutlarına veya gönderim sıklığına göre filtrelenebilir. Bu filtreleme işlemini yapan bir güvenlik duvarı yapılandırması tasarlanabilir. Bunun dışında belirli bir süre içerisindeki toplam belirli boyuta sahip paketlerin kabulü gibi sınırlamalar konulabilir [18].

1.6 UDP

User Datagram Protocol'ün (Kullanıcı Veribloğu İletişim Kuralları) kısaltılmışı olan UDP güvenilir bir protokol değildir. TCP'den farklı olarak bu protokol paketlerin ulaşacağı garantisini veremez. Ses ve görüntü gibi veri gönderimlerinde kullanılmaktadır. Bunun dışında TCP'den diğer bir farkı daha hızlı veri aktarımı sağlar. TCP verinin ulaşacağını garanti ettiği için verinin hedefe ulaşıp ulaşmadığının kontrolünü de yapmaktadır. Bu protokol ulaşım katmanında yer almaktadır [21].

1.6.1 UDP Saldırıları

- **UDP Flood Saldırısı:** UDP Flood Saldırısında saldırgan hedef cihaza çok sayıda UDP paketi gönderir. Bunun sonucunda hedef cihazın kaynakları her gelen UDP paketini kontrol edip yanıtlamak zorunda kaldığı için tükenir ve çalışamaz hale gelir [22].

1.6.2 UDP Saldırıları Önlemleri

UDP Flood saldırısı için alınabilecek önlemlerden biri ICMP paketlerinin yanıt hızını kısıtlamaktır. Çoğu işletim sistemine uygulanan yöntem budur. Fakat bu kısıtlama meşru paketleri de etkiler [22].

1.7 ARP

Address Resolution Protocol'ün (Adres Çözümleme Protokolü) kısaltılmışı olan ARP protokolü IP adreslerini MAC (Media Access Control) adreslerine çevirir. MAC adresi her cihaz için benzersiz olan fiziksel adres olarak açıklanabilir. İletişim kurmak istenen cihazın fiziksel adresinin bilinmesi gerektiğinden bu işlemde ARP protokolü kullanılır. Bu protokolde

yanıtın yetkili birinden geldiği garantilenmez. Ana bilgisayarlar tarafından hiç istek gönderilmemiş olsa bile gelen yanıtların reddedilmemesi güvenlik açığı yaratacağından saldırılara olanak tanır. IPv4 protokolü ARP protokolünü kullanmaktadır. IPv6 ise bunun yerine NDP protokolünü kullanmaktadır İnternette hala yaygın olarak IPv4 kullanıldığı için ARP da kullanılmaya devam etmektedir. Bu protokol ağ katmanında yer almaktadır [23].

1.7.1 ARP Saldırıları

- **ARP Zehirlenmesi (ARP Spoofing):** Yalnızca ARP protokolünü kullanan ağlarda meydana gelen bu saldırılarda saldırgan MAC adresini başka bir cihazın IP adresiyle eşleştirir. Daha sonra hedefe sahte ARP mesajları gönderir. Saldırganlar bu saldırı ile trafiği yönetebilir, verileri ele geçirebilir veya bu saldırı hizmet verememe durumu, ortadaki adam (MitM), oturum ele geçirme gibi birçok saldırı için ortam yaratabilir. Başka bir IP ile bağdaştırma işlemi sayesinde saldıranlar kendilerini gizli tutabilirler [24].

1.7.2 ARP Saldırıları Önlemleri

ARP saldırılarını önleyebilecek birkaç yöntem mevcuttur. Bunlardan ilki VPN kullanmaktır. Şifreli bir şekilde İnternete bağlanmak saldırgan için iletişimi değersiz kılar. Bir diğeri ise Statik ARP kullanmaktır. Bu protokolde ARP yanıtlarının dinlenmesini engelleyecek bir IP adresine statik bir ARP girişi tanımlanabilir. Bir diğer önleme yöntemi ise ARP paketlerine uygulanan filtreleme ile zehirli ARP paketlerini tespit edip durdurmaktır. İmkân varsa bir saldırı gerçekleştirerek sistem ölçülebilir. Saldırının gerçekleşmesi halinde sistem açıklıkları tespit edilip düzeltilebilir [23].

KAYNAKÇA

1. Karimkhani, R. (2018). DNS (DOMAIN NAME SYSTEM) NEDİR VE NASIL ÇALIŞIR? https://medium.com/@ramin_karimhani/dns-domain-name-system-nedi%CC%87r-ve-nasil-%C3%A7ali%C5%9Fir-465513138670
2. What is DNS cache poisoning? | DNS spoofing (t.y) https://www.cloudflare.com/learning/dns/dns-cache-poisoning/
3. DNS attack. (2021). https://www.techtarget.com/searchsecurity/definition/DNS-attack
4. What is DNS fast flux? (t.y) https://www.cloudflare.com/learning/dns/dns-fast-flux/#:~:text=DNS%20fast%20fluxing%20is%20a%20technique%20that%20involves%20associating%20multiple,of%20IP%20addresses%20are%20used.
5. Taylor, R. (2021). Four major DNS attack types and how to mitigate them. https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/
6. SYN Flood Saldırıları. (2021). https://www.priviasecurity.com/syn-flood-saldirilari/
7. SYN saldırısı. (2020). Vikipedi. https://tr.wikipedia.org/wiki/SYN_sald%C4%B1r%C4%B1s%C4%B1
8. Heaton, R. (2020). How does a TCP Reset Attack work? https://robertheaton.com/2020/04/27/how-does-a-tcp-reset-attack-work/
9. TCP reset attack. (2022). Wikipedia. https://en.wikipedia.org/wiki/TCP_reset_attack#:~:text=TCP%20reset%20attack%2C%20also%20known,a%20forged%20TCP%20reset%20packet.
10. Arampatzis, A. (2021). What is Session Hijacking? https://www.venafi.com/blog/what-session-hijacking
11. Doğan, S. (2021). Syn Flood Nedir? Nasıl Önlenir? https://mertmekatronik.com/syn-flood-nedir#syn-nasil-onlenir
12. Şen, İ. (2018) Oturum Ele Geçirme (Session Hijacking). http://ismailsen.com.tr/oturum-ele-gecirme-session-hijacking/
13. What is IP spoofing? (t.y.) https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/
14. File Transfer Protocol. (2022). Wikipedia

https://en.wikipedia.org/wiki/File_Transfer_Protocol

15. Top 4 FTP Exploits Used by Hackers. (2018). https://www.globalscape.com/blog/top-4-ftp-exploits-used-hackers
16. Bir FTP Sunucusuna Yapılabilecek Saldırı Türleri. (2013). https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/bir-ftp-sunucusuna-yap%C4%B1labilecek-sald%C4%B1r%C4%B1-t%C3%BCrleri
17. 10 Essential Tips for Securing FTP and SFTP Servers. (2017). https://www.helpsystems.com/blog/10-essential-tips-securing-ftp-and-sftp-servers
18. Yanmış, S. (2019).ICMP NEDİR. https://siberguvenligi.blogspot.com/2019/11/icmp-nedir.html
19. Smurf attack. (2022). Wikipedia https://en.wikipedia.org/wiki/Smurf_attack
20. Lutkevich, B. (2021). ICMP (Internet Control Message Protocol) https://www.techtarget.com/searchnetworking/definition/ICMP
21. UDP. (2021). Vikipedi https://tr.wikipedia.org/wiki/UDP
22. What is a UDP flood attack? (t.y) https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/
23. Klepfish, N. (2022). ARP Spoofing https://www.imperva.com/learn/application-security/arp-spoofing/
24. ARP Zehirlenmesi. (2020). Vikipedi https://tr.wikipedia.org/wiki/ARP_zehirlenmesi