BİLGİSAYAR AĞLARI ÜZERİNDE İLETİLEN VERİLERE ZARAR VERMEK İÇİN KULLANILAN ÖNEMLİ TEKNİKLER ve KORUNMA YOLLARININ İNCELENMESİ

Fatma AKGÜN[1] Ercan BULUŞ[2] Şenol ŞEN[3]
[1,2,3] Bilgisayar Mühendisliği Bölümü
Mühendislik-Mimarlık Fakültesi
Trakya Üniversitesi, 22100, Edirne
[1]e-posta: fatmaa@trakya.edu.tr [2] e-posta: ercanb@trakya.edu.tr
[3]e-posta: senols@trakya.edu.tr

Anahtar Sözcükler: Saldırı(Attack), Güvenlik(Security), Paket Koklama(Sniffing), Aldatma(Spoofing).

ÖZET

Güvenlik hayatımızdaki en önemli kavramlardan biridir. Son yıllarda teknolojinin bu kadar hızlı bir biçimde gelişmesiyle beraber ağ üzerinden veri iletiminde çeşitli güvenlik açıkları ortaya çıkmıştır. Bu çalışmada, bu tür güvenlik açıklarının nasıl ortaya çıkabileceği ve bu tür durumlardan korunmak için neler yapılabileceği hakkında bilgi verilmiştir. Bu bilgiler ışığında, çağımızın gerektirdiği düzene uygun olarak bilgiler bir bilgisayardan diğer bilgisayara, kısaca bir beyinden diğer bir beyine güvenli bir şekilde ulaşabilecektir.

1. GİRİŞ

Günümüzde teknolojinin hızlı gelişmesiyle beraber güvenlik açıkları da bir o kadar artmıştır. Veriler bir ortamdan diğer ortama aktarılırken her an çalınma, değişime uğrama ya da yok edilme tehlikesi ile karşı karşıyadır. Veri paketleri network cihazları vasıtasıyla ağ üzerinden aktarılırken, kötü amaçlı kişiler bu cihazları ve bilgisayarları paket koklama(sniffleyerek) ya da aldatma(spoofing) işlemleri yaparak bilgileri ele geçirebilirler.

Saldırganlar bu cihazların IP/MAC tablolarının tutulduğu ARP(Adres Çözümleme Protokolü) [1] belleklerini zehirleyerek, kısaca kandırarak paketlerin kendilerine ulaşmasını sağlayabilirler. Saldırgan ele geçirdiği paket üzerinde değişimler yaparak bunu gerçek alıcısına gönderebilir. Yapılan bu işlemlerden ne göndercinin nede alıcının haberi olmayacaktır. Tüm iletim boyunca kendi aralarında haberleştiklerini sanacaklar ve saldırgan kendini aradan çekip bilgisayarların ARP belleklerini eski haline getirmesiyle aldatma işlemi son bulacaktır.

2. PAKET KOKLAMA

2.1 Paket Koklama Nedir?

Ağ üzerinde iletilen verilerin çalınması işlemine paket koklama denir. Bir paket koklayıcı ağ üzerindeki tüm trafiği kontrol etmek için bilgisayar içerisine yerleşir ve kendi kendine çalışır. Bunlar yazılımsal ya da donanımsal olabilir [2]. Birçok koklayıcı, ayrımsız tür olarak adlandırılan "promiscuous mode"[3] özelliğine sahip ethernet kart modülü vasıtasıyla kendileri haricinde diğer kullanıcılara iletilen paketleri de izinsizce ele geçirip, işleyebilirler. Bazı UNIX bilgisayarlarda tek bir komut satırı yazarak bilgisayarın ayrımsız tür ile çalışması sağlanabilir.

2.2 Paket Koklayıcılarının Çalışma Ortamı

İki farklı çalışma ortamı bulunmaktadır [4,5].

2.2.1 Paylaşımlı Ortam(Shared Ethernet):

Bu ortamda tüm kullanıcılar hub sayesinde paket alımı ve gönderiminde ortak bir ağ yapısı kullanarak haberleşirler ve bant genişliği için rekabet ederler. Bu yapıda ayrımsız tür özelliğine sahip ethernet kartları kullanılarak veriye gizlice ulaşılabilir. Yapılanlardan ne alıcının nede göndericinin haberi olmaz.

2.2.2 Anahtarlamalı Ortam(Switched Ethernet):

Bu ortamda ise tüm bilgisayarlar hub yerine switch vasıtasıyla haberleşirler. Switch her bir bilgisayarın MAC [6] (Ortam Erişim Kontrolü) adresini yani fiziksel ethernet adresini bir tabloda saklar. Swichler tüm ağda broadcast yayın yapmazlar, ellerindeki CAM'e (İçerik Adresleme Tablosu) tablolarına bakarak iletimlerini gerçekleştirirler ve her bir porta belirli bir MAC adresi tahsis edildiğinden bu yapı sayesinde iletimlerini gerçekleştirirler. Bu ortamda da switche çok fazla istek gönderip onun gelen isteklere cevap veremeyip, hub modunda çalışmaya başlamasına ve paketleri tüm kullanıcılara broadcast olarak aktarmasına neden olunabilir.

2.3 Koklama Türleri

2.3.1 IP Tabanlı Koklama:

Hub ortamında ya da bus topolojili bir ortamda herhangi bir bilgisayara ayrımsız tür özelliğini içeren bir kart takılarak koklama işlemi gerçekleşir. Saldırgan ele geçirdiği paketin hedef adreslerinde filtrelemeler yaparak, koklama işlemini gerçekleştirir. Bu işlem sadece switchsiz ortamlarda yapılabilir.

2.3.2 MAC Tabanlı Koklama:

Bu ortamda da yine ayrımsız tür özellikli ethernet kartına sahip bilgisayar, mevcut yazılım vasıtasıyla elde ettiği paketi değişime uğratabilir. Paketler üzerinde ilgili alıcıların MAC adresleri filtrelenerek tüm paketler koklanabilir. Bu işlemler IP tabanlı koklamada olduğu gibi switchsiz ortamlarda gerçekleştirilebilir.

2.3.3 ARP Tabanlı Koklama:

Bu metot diğerlerine oranla biraz farklı işlem görür. Burada koklama yapacak bilgisayar switchli ortamda çalıştığından, ayrımsız tür özelliğinde olan bir ethernet kartına sahip olmasına gerek yoktur. Burada yapılan işlem; switchler üzerindeki IP/MAC tablolarının saldırganlar tarafından yanlış ARP cevapları ile doldurulması ya da çok fazla istek alan switchin hub modunda çalışması sağlanarak koklama yapılır. ARP [1] (Address Resolution Protocol) protokolü, IP'nin hizmetlerini kullanmaz o nedenle IP başlığı içermez. ARP paketi, sadece yerel ağ üzerinde hazırlanıp gönderilir. Uzak ağlardaki (yönlendiricilere bağlı ağlar) kullanıcıların fiziksel adresini bilmek bir anlam ifade etmez. Çünkü yönlendiriciler fiziksel adreslere göre değil ağ katmanı mantıksal adresine göre (IP adresi) yönlendirme yapar. Bu yüzden routerlar üzerinde ARP kandırması yapılamaz.

2.4 Paket Koklayıcının Kullandığı Araçlar:

Bir paket koklayıcı ağ üzerinde herhangi bir açık olup olmadığını anlamak ve verileri ele geçirip işlem yapabilmek için, Hata Analizi Cihazı, Veri Yakalama Cihazı, Tampon Bellek, Performans Analizci, Kod Çözücü, Paket Düzenlemesi ve Aktarılması gibi çeşitli cihazlar kullanmaktadır[11].

2.5 Paket Koklayıcılarının Kullanım Amacı:

2.5.1 Yöneticilere Yardımcı Koklayıcılar:

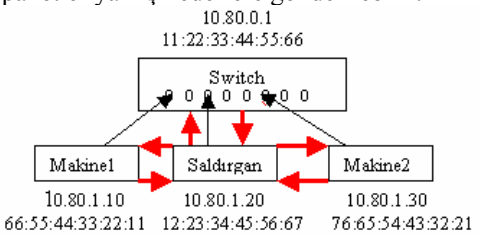
Paket koklayıcının bir ağda kullanılması LAN/WAN yöneticilerine ağ trafik analizi ve ağda bir problem olmuşsa bunun nerede olduğunun tanımlanmasını sağlar. Birçok koklayıcı kullanılıp sistem kontrol altına alınabilir. Bu şekilde bir paket koklayıcı hata ve performans analizi yapabilir. Hata analizinde ağdaki problemler bulunur, performans analizinde ise ağ tıkanıklıkları bulunabilir. Ayrıca paket koklayıcı, ağa zorla girmek isteyen kişileri ağ yöneticilerine bildirir.

2.5.2 Saldırganlara Yardımcı Koklayıcılar:

Saldırgan gibi kötü amaçlı kişilerin sistem üzerinde zarar vermek amacıyla kullandıkları programlardır. Bu şekilde ağda iletilen paketler ele geçirilip sistemlere büyük zararlar verilebilir.

3. ALDATMA

Ağ üzerinde iletilen bilgiyi çalmak için bilgisayarlar ve ağ cihazları üzerinde çeşitli işlemler yapılıp, paketler yanlış hedeflere gönderilebilir.



Şekil–1. Switchli ağlardaki aldatma işlemi

Şekil–1 de olduğu gibi veriler ilgili portlara gönderilirken, aradaki saldırgan switchin ARP belleğini zehirleyerek her bir bilgisayara iletilen bilgilerin kendi üzerinden gitmesini sağlayabilir. Kırmızı bağlantılarla gösterildiği gibi iletim saldırgan bilgisayar üzerinden gerçekleşir.

3.1 ARP Aldatmacası

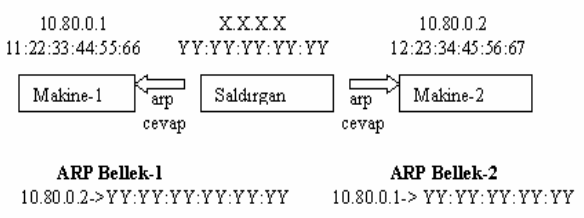
Burada; ARP belleğinde IP/MAC adresleri eşlemesini yanıltarak ARP aldatmacası gerçekleştirilmektedir [7]. Ağ trafiğini bir ya da daha fazla bilgisayardan saldırganın bilgisayarına yönlendirebiliriz. Amaç; kendini hedef aldığı bilgisayarlara ağ geçidi gibi gösterip tüm paketleri ele geçirmektir. Burada saldırgan ARP tablosu üzerinde yönlendirici için tahsis edilen alana kendi MAC adresini yazdırarak ya da FF:FF:FF:FF:FF:FF adresini girerek paketlerin herkese gitmesini sağlayabilir. Bu saldırı ile hedef bilgisayarın önbelleği zehirlenir. Saldırgan kendisini geçit (gateway) bilgisayar olarak tanıttığından, ağ üzerinde geçit bilgisayara gönderilen tüm paketleri ele geçirir. Burada olan işlemi ne geçit bilgisayar nede kurban bilgisayar anlamayacaktır ve iletim devam edecektir. Bu işlemleri yapmak için güçlü yazılımlar vardır. Öncelikle kurban bilgisayardan ağ geçidine bir "traceroute" çekilir ve paketin nerelerden hangi hızla iletildiğine bakılır. Buna ek olarak "arp –a" ile kurban bilgisayarın ARP belleği kontrol edilir. Bu işlemlerden sonra saldırgan bilgisayar ilgili yazılımı çalıştırarak kurban bilgisayarın trafiğinin kendi üzerinden akmasını sağlar.

3.1.1 Ortadaki Adam Saldırısı(Man-in-the-middle Attack):

Hub ortamında bir bilgisayar diğerine veri gönderdiğinde, saldırganda hub'a bağlı ise bu gönderilen paketi alıp inceleyebilir ve birçok bilgiye ulaşabilir. Switchler ise IP/MAC tablolarını karşılaştırarak hangi frame'in hangi porta gideceğine karar verir. Bu tablo switch açıldığında devreye girer ve IP/MAC adreslerini kontrol eder.

"Ortadaki Adam" saldırısı, ARP Aldatmacası'nın farklı bir modelidir. Bu saldırıda; saldırgan hedef iki bilgisayar arasındaki iletişimi ele geçirmek üzere kendini araya ekler. Bu şekilde bir koklama işlemi gerçekleşmiş olur. Verilerin iki hedef arasında

doğrudan iletilmesi yerine, saldırgan üzerinde değişime uğratılarak gönderilir. Fakat bu işlemi iki bilgisayarda anlayamaz. Çünkü saldırgan her iki bilgisayarın da ARP belleklerini zehirlemiştir. Saldırgan burada; A ve B bilgisayarlarının ARP belleklerini zehirler. A'nın IP/MAC tablosunda B için, B'nin ip adresi ve saldırganın MAC adresi kayıtlıdır. B'nin IP/MAC tablosunda ise A için, A'nın ip adresi ve saldırganın MAC adresi kayıtlıdır. Bu işlemlerden sonra A ve B bilgisayarlarının arasındaki bütün IP trafiği, doğrudan birbirlerine gitmesi gerekli iken ARP bellekleri zehirlendiği için şekil–2 de olduğu gibi öncelikle saldırgan bilgisayara gider.



Şekil–2. Ortadaki adam saldırısı

3.2 IP Aldatmacası

IP paketlerindeki kaynak IP adresini değiştirerek ya da vekil sunucular vasıtasıyla diğer sitelerde işlem yaparak IP Aldatmacası yapılabilir [8]. TCP/IP protokolleri üzerindeki IP adresini yanlış göstererek bu işlemi gerçekleştirebiliriz. IP aldatmacası iki şekilde yapılabilir.

1-) Proxy/Socks sunucularını kullanarak,
2-) IP paketlerinde düzenlemeler yaparak,

Proxy/Socks sunucularını kullanmak diğerine oranla daha basit bir yöntemdir. IP paketlerini düzenleyerek yapılan aldatma ise çok daha etkilidir. Genel DDoS saldırılarında ve oturum hırsızlığında (session-hijacking) kullanılır [9].

3.2.1 Proxy/Sock Sunucularını Kullanmak:

Internet'te sitelerin bizim ip adresimizi tutmaması için, kullandığımız tarayıcının bağlantı ayarlarını yaparak, bu sitelere bir vekil (proxy) sunucu üzerinden bağlanabiliriz. Böylece hedef site bizim ip'imizi değil de vekil sunucunun ip'sini kayıtlarında tutar, eğer vekil sunucu ip'mizi saklama özelliğine sahip değilse, ip'mizi hedef bilgisayara gönderir. Ya da hedef sitenin sistem yöneticisi bu vekil sunucunun loglarına (kayıtlarına) bakarak ip'mizi ele geçirebilir. Socks sunucusu vasıtasıyla da ftp, telnet vs. işlemleri güvenle gerçekleştirebiliriz. Ama hedef site eğer Socks sunucusu ile bağlandığımızı anlarsa bağlantıyı kesebilir.

3.2.2 IP Paketlerini Düzenlemek:

Burada önce hedef bilgisayar seçilir, sonra güvenilir bir bilgisayar ile güven ilişkisi bulunur. Güvenilen bilgisayar yapılan binlerce icmp isteğine cevap veremediğinden kapanır ve hedefin TCP sıra numaraları örneklenir. Güvenilen bilgisayar sahiplenilip, sıra numaraları elde edilir. Eğer başarılı olursa, saldırgan 'arka kapı' bırakmak için basit bir komut çalıştırır. Hedef bilgisayar; güvenilen bilgisayar ile ilişki kurduğunu düşündüğünden ona cevaplar gönderecektir, fakat güvenilen bilgisayar SYN Flooding saldırıları ile meşgul olduğundan bu isteklere yanıt döndüremeyecektir. Saldırgan bu paketlerin TCP sıra numaralarını elde edip iletişimi kendi üzerinden sağlayacaktır. Bu durumdan yararlanan saldırgan kendince sahte tahmini cevaplar göndererek iletişimini gerçekleştirecektir. Buna pasif aldatmaca denir. Bunun yanı sıra saldırgan iç ağda ise gelen bu paketleri koklayarak bu verilere ulaşabilecektir ve kendince doğru cevaplar göndererek hedef bilgisayarı aldatıp, işlem görecektir. Bu işleme aktif aldatmaca denmektedir.

3.3 MAC Aldatmacası

MAC adreslerinin fiziki olarak değiştirilmesi ve ip adreslerindeki değişiklikler ile MAC aldatmacası yapılabilir. MAC aldatmacası, ARP aldatmacasından biraz farklı olarak gerçekleşir. Çünkü burada ARP tabloları sabitlenmiş durumdadır, bunlar üzerinde bir işlem yapılmasına gerek yoktur. MAC Aldatmacası gerçekleştirilirken, SYN Flooding saldırısı ya da genel olarak DoS aracılığıyla kurban bilgisayar offline durumuna getirilir. Daha sonra saldırgan bilgisayar, kendi bilgisayarının MAC ve IP adreslerini kurban bilgisayarın MAC ve IP adresleriyle değiştirir. Böylece de kurban bilgisayara gelecek bütün trafik saldırgan bilgisayara gelmiş olur. Bunu yapmanın birkaç yolu vardır.

Kendimiz adres değişikliği yapabiliriz. Ağ üzerinde bir ethernet frame gönderdiğimizde yazılım vasıtasıyla bu alana müdahale edip, tekrardan konfigüre edebiliriz. Bazı kartlar Windows'taki denetim ayarları vasıtasıyla MAC adreslerini düzenlemeye yardımcı olur. Kart içerisindeki adresi yenileyebiliriz. Bunun için kullanılan chipset'in özelliklerini bilen bir yazılıma ihtiyaç duyup, kart üzerine yeni bir adres atanması sağlanabilir. Anakart üzerindeki dahili ethernet kartlarının MAC adresleri de BIOS ayarlarından değiştirilebilir. Linux kullanıcıları aldatma yazılımı olmaksızın "ifconfig" gibi tek bir parametre kullanarak MAC adreslerini değiştirebilir.

3.4 DNS Aldatmacası

DNS sunucularını ele geçirerek veya sorgulara sahte cevaplar vererek DNS aldatmacası yapılabilir. DNS (Domain Name Server) alan adlarını ip'ye ya da ip'yi alan adına çevirmekte kullanılan güvenli bir protokoldür. Bu protokol, cevapları ve talepleri eşleştirmek için bir kimlik sahası içerir. DNS aldatmacasında amaç cevapları DNS sunucusundan önce belirlemektir. Bu belirleme işlemi yerel olarak ağı koklamayla ele geçirilebilir. Uzaktan erişimlerde işlemler daha zor olmaktadır. Örneğin saldırganın bir siteyi kontrol altına aldığını düşünürsek, istek yapacağı hedef DNS sunucusu da tahmin edilebilir

sıra numaralarına sahip ise işlemler oldukça kolaylaşır. (Sıra numaraları her defasında bir arttırılmış olmalıdır.)

3.4.1 DNS Önbellek Zehirleme:

DNS Sunucuları bir önceki sorguya verdikleri cevabı bir süreliğine saklamak için önbellek kullanırlar. Her defasında talep yapılan alandan yetki almakla vakit kaybetmemek için bunu yaparlar. DNS aldatmacası bu önbelleği zehirleyerek yanlış bilgi göndermesini sağlamaya yöneliktir.

4. SONUÇ

Yapılan araştırmalar göstermiştir ki her alanda, mevcut yapıyı kötüye kullanma isteği vardır. Bu tür saldırılardan dolayı sistemler büyük ölçüde zarar görmektedir. Donanımsal güvenlik oluşturmanın yanında yazılımsal güvenlikte sistemler üzerinde büyük ölçüde fayda sağlamıştır. Switchler ve mevcut bilgisayarlar üzerinde gerekli yapılandırılmalarla dinamik ARP bellek güncellemeleri yerine statik güncelleme yapılıp bu işlemler tarih ve saate göre loglanmalıdır [10]. Bazı switchler üzerinde bulunan administrator portunu iyi yapılandırarak belirli portlara belirli kişilerin erişimi sağlanılıp konfigüre edilmelidir. DHCP Server kullanımında dikkatli davranılmalı ya da hiç kullanılmamalıdır. Çünkü bu şekilde her bir bilgisayara farklı bir ip adresi tahsisi yapılacağından, IP/MAC tabloları sürekli değişecektir.

Hub kullanmak, yerine switch kullanımına geçilmelidir. Fakat switchler üzerinde de aldatma işlemi gerçekleştirilip, verilerin yetkisiz kişiler tarafından koklanmaması veya değişime uğramaması için kaliteli switchlerin kullanımına özen gösterilmelidir. Domain yapısına geçip, kullanıcıların bilgisayarlarını yöneticinin belirlediği yetkiler dahilinde kullanmaları sağlanılabilinir. Bu yapıda kullanıcıların hiçbir programı kurmasına izin verilmeyerek, güvenlik sağlanabilir. Bu daha çok öğrenci laboratuarlarında ve kritik işlemler yapan bilgisayar kullanıcılarında uygulanması yerinde olacaktır. VLAN (Sanal Yerel Ağ-Virtual Local Area Network) yapısına geçerek ağda herkesin kendi yerel hattını kullanmasıyla, ağ üzerinde daha verimli bir yapı sağlanabilir.

Router ve firewall gibi ana cihazlar üzerinde bazı kısıtlamalar getirilmelidir. Bunun için bu cihazlar üzerindeki yapılandırmalarda gerekli access-list'ler oluşturmak gerekir. Sunucular, routelar, firewall'lar, switch'ler vs. tüm ağ cihazları üzerinde güvenlik önlemleri en başından uzmanlarca yapılıp, herhangi bir güvenlik açığına meydan bırakılmamalıdır.

Ters sorguları aktif hale getirmek gerekmektedir (RDNS, RARP vb.). Koklayıcıları bulmak için Ping-1 metodu, Ping-2 metodu, DNS metodu, ARP metodu, Tuzak metodu, Kaynak Yönlendirme metodu, Gizlilik metodu, Zaman Ölçümü, SNMP İzlenimi, Antisniffer programları kullanılarak tespit işlemi yapılabilir [11]. Genel korunma yolları olarak SSL [12], PGP [13] and S/MIME, SSH [14], VPN [15], Şifreleme[16,17], Kerberos [18], Tek Zamanlı Şifreleme işlemleri yapılabilir.

KAYNAKLAR

[1] Wagner R., Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks, SANS Institute, August 2001.

[2] Dhar S., Sniffers Basics and Detection, version 1.0-1, Information Security Management Team, 2002.

[3] Daiji S., Detection of Promiscuous Nodes Using ARP Packets, August 2001.

[4] Danielle L., Sniffing, SANS Security Essentials (GSEC), June 1, 2001.

[5] Velasco V., Introduction to IP Spoofing, SANS Institute 2000-2002, November, 2000.

[6] Cardenas E. D., MAC Spoofing—An Introduction, CIAC Security Essentials Certification (GCEC), 23 August 2003.

[7] Siles R., Real World ARP Spoofing, August 2003.

[8] V.Tripunitara M., Dutta P., A Middleware Approach to Asynchronous and Backward Compatible Detection and Prevention of ARP Cache Poisoning, 15th Annual Computer Security Applications Conference December 6-10, 1999 Phoenix, Arizona.

[9] Perring A., Song D., Yaar A., StackPi: A New Defense Mechanism Against IP Spoofing and DDoS Attacks, School of Computer Science Carnegie Mellon University, Pittsburgh, PA 15213, February 2003.

[10] Spangler R., Packet Sniffer Detection with AntiSniff, University of Wisconsin, Department of Computer and Network Administration, May 2003.

[11] Graham R., Sniffing, http://www.robertgraham.com/pubs/sniffing-faq.html, April 2000.

[12] Kriptografi, http://sertifika.bilten.tubitak. gov.tr/net/teknik/kriptografi.jsp#1.13.

[13] Levi A., Çağlayan U., Elektronik Posta Güvenliği İçin PGP Kullanımı, http://mercan. cmpe.boun.edu.tr/~levi/AS97.HTM.

[14] SSH Nedir?, http://security.nyg.ege.edu.tr/ ssh/SSH_nedir.htm.

[15] VPN (Virtual Private Network), http://www.devel.gazi.edu.tr/modules.php?name=News&file=article&sid=52.

[16] Stinson D. R., Cryptography: Theory and Practise, Second Ed., CRC Press, 2002.

[17] Sakallı M. T., Buluş E., Tutanescu I., Security and DSPs in VoIP (Voice over IP) Networks, ELECO 2003, 3th International Conference on Electrical and Electronics Engineering, Bursa, Turkey, 2003.

[18] Karabacak B., Kerberos, http://www. devel.gazi.edu.tr/modules.php?name=News&file=article&sid=52.