BİR YEREL ALAN AĞINI GİZLİCE İNTERNETE AÇMAK (HTTP ÜZERİNDEKİ SANAL YEREL AĞ)

Yüksel ARSLAN
Mikes A.Ş, Çankırı Yolu 5.km Akyurt/Ankara
yuksel.arslan@mikes.com.tr

Abstract

Nowadays computers and computer networks are used every field of our lives. Internet is now profound. Organizations, companies and ordinary people store proprietary, confidential and private data on computers. It is therefore very important that unwanted, malicious people do not access this data.

Firewalls, intrusion detection and prevention systems, anti-virus software are used for computer and computer networks security. They are developed continuously. These tools are generally to protect networks from outside attackers. Information systems security tools to protect attacks coming from inside are very limited and most of them are not effective.

In this paper it is shown how a LAN is opened to internet secretly via an insider attack. An outside computer on the internet will be part of the local area network despite all of the security tools. The attacker uses here a private second IP address uncommonly to be part of the LAN.

Key words: Insider threat, tunneling, VPN (Virtual Private Network), firewall, intrusion detection and prevention system.

1. Giriş

Bilgi sistemlerine yapılan saldırıları organize ve organize olmayan saldırılar ile dışardan yapılan ve içerden yapılan saldırılar olmak üzere dört gruba ayırabiliriz [1].

İçerden saldırı yapan kişiler, çalışmakta olan veya daha önce çalışmış işçiler, müteahhitler, iş ortakları olabilir. Bunların yerel ağ kaynaklarına halihazırda veya geçmişte ulaşma hakkı olmuş olabilir. Bu kişilerin şirket içi politikalar, süreçler ve uygulamalar hakkında bilgisi vardır ve bu bilgilerini, bazen de şirket dışındaki kötü niyetli kişilerle ortaklık yaparak saldırılar düzenlemek için kullanırlar [2].

Bugün yaygın şekilde kullanılan bilgi güvenliği sistemleri; ateşduvarları, sızma tespit ve önleme sistemleri aslında bir yerel alan ağını dışardan gelen saldırılara karşı korumaktadır. Bunun farkında olan saldırganlar saldırıyı içeriye sızarak içerden gerçekleştirmektedirler veya daha önce belirttiğimiz yerel alan ağı üzerindeki kaynaklara erişim hakkı olanlar saldırıyı gerçekleştirmektedir.

1997'de ABD Savunma Bakanlığı'na yapılan saldırıların %87'si içerden yapılan saldırılardır. 2004 yılından 2006 yılına kadar yapılan çalışmalarda içerden yapılan saldırıların %31'den %27' düşmüş olduğu görülse de parasal açıdan daha büyük zarar vermişlerdir [3].

Yazılan truva atları, solucanlar, ajan programların hepsi saldırıyı içerden gerçekleştirir. Bu programların içeri sokulması ise çok da zor olmamaktadır. E-mail ekleri ve ziyaret edilen sitelerden kolayca kendi bilgisayarımıza gelebilmektedirler.

Bu makalede içerden gerçekleştirilen bir saldırı ile bir yerel alan ağının bütünüyle internete nasıl açıldığı anlatılıyor. Bu SÖA (Sanal Özel Ağ) (VPN, Virtual Private Network) teknoloji bilgisi, Windows işletim sistemi TCP/IP kolaylıkları kullanılarak ve ateşduvarı sistemi alt edilerek çok da zor ve karmaşık olmayan bir istemci/sunucu tasarımı ve gerçeklemesiyle gösteriliyor.

Bu saldırı gerçekleştiğinde internete bağlı bir bilgisayar saldırı gerçekleştirilen yerel alan ağına bağlı bir bilgisayar haline gelmektedir. Bu duruma geldikten sonra saldırganın diğer saldırı tekniklerini de kullanarak bu ağda istediği bilgiye sahip olması çok kolay olacaktır.

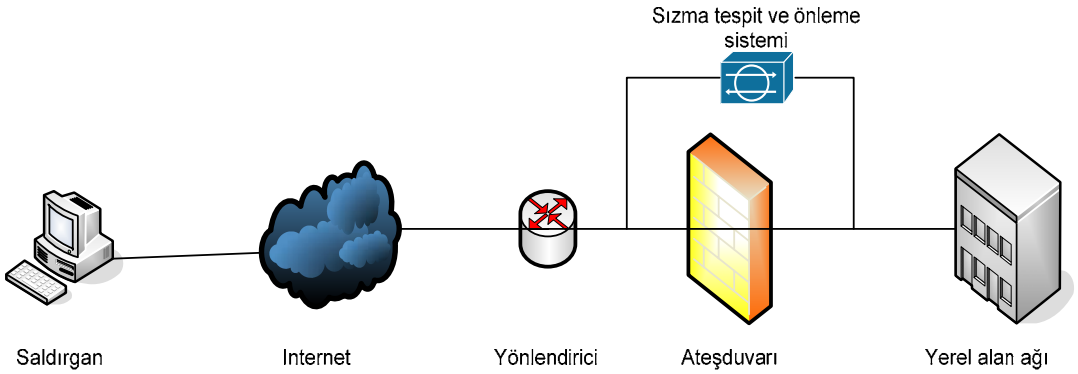
Bundan sonra sırasıyla amaç, Windows işletim sistemi tabanlı bir yerel alan ağının işimize yarayacak özellikleri, amacımıza ulaşmak için tasarlanan çözüm, gerçekleme ve testinden sonra çıkarılan sonuç açıklanacaktır.

2. Amaç

Yerel alan ağları genelde bir ateşduvarının arkasında bulunurlar. İnternete çıkmak için tek bir IP adresi kullanırlar. Bu IP adresi yerel alan ağında bulunan tüm kullanıcılar için ortaktır, yani herkes bu IP

adresini kullanarak internete çıkabilir. Yerel alan ağında kullanılan IP adresleri özel IP olarak adlandırılır ve internet üzerinde bu IP adreslerinin kullanılmasına izin verilmez. Ateşduvarı prensip olarak yalnızca bazı TCP/UDP kapılarına (port) içerden dışarıya doğru yapılacak bağlantılara izin verir; ancak dışardan içeriye yapılacak hiçbir bağlantıya izin vermez. Bu kural, tüm yerel alan ağı için tek internet IP adresi ile birleştiğinde, dışardan içerdeki herhangi bir makineye direk saldırı olasılığını en aza indirger. Şekil 1'de internet üzerindeki bir saldırgan ile yerel alan ağı arasındaki cihazlar gösteriliyor.

Bizim amacımız internet üzerinden, ateşduvarı arkasındaki bir yerel alan ağının tüm kaynaklarına nasıl erişilebildiğini göstermek. Windows işletim sistemi (testlerde Windows XP kullanılmıştır) kullanılan bir yerel alan ağına internet üzerinden bir saldırgan bağlanacak ve bu ağın bir parçası olacaktır. Bunu yapan çeşitli SÖA (VPN) istemci/sunumcu yazılımları vardır. Bu programlar ateşduvarı ve/veya yönlendirici üzerinde çeşitli ayarlar yapmayı ve/veya özel donanım kullanmayı gerektirir [4]. Yalnızca sistem yöneticisi tarafından çalışması sağlanabilir. Bu nedenle daha önce açıkladığımız iç saldırganlar tarafından kullanılamazlar. Yine bu tür programlar kendi grafik arayüzleri ile yerel alan ağını kullanıcılara gösterirler. Burada anlatılan çözümde Windows işletim sisteminin kendi arayüzleri kullanılmaktadır. Bağlantı yapılan yerel alan ağı, saldırgan bilgisayarın ağ komşularımda, yerel alan ağına bağlıymış gibi görüntülenmektedir. İnternet üzerinden bağlanan saldırgan bilgisayarının yerel alan ağına bağlı bilgisayardan bir farkı kalmamaktadır. Bunu yaparken de ateşduvarı ve/veya yönlendirici üzerinde ayar yapmaya gerek duymamaktadır.



Şekil 1 İnternete bağlı yerel alan ağındaki cihazların bağlantısı

3. Windows İşletim Sistemi Tabanlı Yerel Alan Ağı

Bilgisayarların kablolarla birbirine bağlanması tek başına bir ağ olma özelliği için yeterli değildir. Bu bilgisayarların birbiriyle haberleşeceği bir haberleşme protokolü olmalı ve bilgisayarlar üzerinde çalışan işletim sistemi bu protokolü kullanarak çeşitli kolaylıklar sağlamalıdır. Bilgisayarları bir ağ haline getirmenin amacı da budur. Aşağıda Windows tabanlı bir işletim sisteminin haberleşme protokolü olan TCP/IP yapılandırması ve en önemli servislerinden biri olan bilgisayar tarayıcı (browser) servisi açıklanacaktır.

3.1. Windows TCP/IP yapılandırması

Windows TCP/IP yapılandırması bir bilgisayara birden fazla IP adresi verilmesine izin verir. Bir bilgisayarda birden fazla IP adresi varsa önce ilk IP adresi, sonra sırasıyla diğer IP adresleri kontrol edilerek paketler alınır ve gönderilir. Örneğin; bir IP adresini pinglediğinizde bu IP adresinin ağ kısmı birinci IP adresinin ağ kısmına uymuyorsa, ikinci IP adresinin ağ kısmıyla karşılaştırılır ve bu böyle devam eder. Ayarlanan IP adreslerinden birinin ağ adresi ile uyuşursa Ping paketi uyuşan IP adresinin ayarlandığı Ethernet arayüzünden gönderilir. Gönderilecek paketin IP adresinin ağ adresi kısmı, bilgisayara verilen IP adreslerinin tamamının ağ adresiyle uyuşmazsa, Ping paketi ayarlanan ağ geçidine gönderilir.

Windows TCP/IP yapılandırmasının bu özelliğinden sunucuda (sunucu ve saldırgan bilgisayarı aynı anlamda kullanılmaktadır) faydalanılmaktadır. Sunucuya ikinci IP adresi verilir. Birinci IP adresi sunucunun internete bağlanmasını sağlarken ikinci IP adresi sunucunun saldırı yapılan yerel alan ağına bağlanmasını sağlar.

3.2. Bilgisayar Tarayıcı (browser) Servisi [5]

Windows işletim sistemi yüklü bir makinede ağ komşularım tıklandığında, ağa bağlı tüm bilgisayarların bilgisayar adları bir pencere içinde görünür. Bu bilgisayar ikonlarından birini tıkladığınızda ise o bilgisayar üzerinde paylaştırılan dizinleri görebilirsiniz. Bunu Windows işletim

sistemi bilgisayar tarayıcı adı verilen bir servis yardımıyla yapar. Ağ üzerinde bulunan tüm bilgisayarlar belirli sürelerde kendi bilgisayar adlarını, paylaştırdıkları kaynakları yayımlarlar (broadcast). Ana tarayıcı olarak seçilen bilgisayar bu yayımların hepsini toplar ve eğer bir bilgisayar ağ kaynaklarını sorgularsa bu bilgileri ona gönderir. Ana tarayıcı da belli aralıklarla ana tarayıcı olduğunu yayımlar, böylece ağ üzerindeki tüm bilgisyarlar ana tarayıcının kim olduğunu öğrenirler.

Anlaşılacağı gibi yerel alan ağındaki tüm bilgisayarları ve paylaştırılan kaynakları görmek bilgisayar tarayıcı servisi aracılığıyla olmaktadır, bu servisin çalışması da yayımlarla olmaktadır. Yayım paketleri bizim işimize yarar. Yayım paketlerini ağ üzerindeki tüm bilgisayarlar görür. İstemci bilgisayarımızda bu paketleri alıp sunucuya göndermekte zorlanmaz.

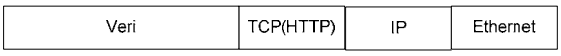
4. HTTP Üzerindeki Sanal Yerel Ağ

4.1. Tasarım ve Gerçekleme

İstemci ve sunucu olarak çalışan iki ayrı yazılım tasarlanmış ve gerçeklenmiştir. İstemci internete açacağımız yerel alan ağına bağlı herhangi bir bilgisayar üzerinde çalışacaktır. Sunucu ise bu ağa internet üzerinden dahil olacak bilgisayar üzerinde çalışmaktadır.

4.1.1. İstemci yazılımı

İstemci yerel alan ağına bağlı herhangi bir bilgisayar üzerinde çalışır ve kendine gelen tüm yayımları (sunucunun yayımları hariç) ve sunucuya adreslenmiş paketleri alarak sunucuya gönderir. Bu gönderme işleminden önce paketi Şekil 2'de görüldüğü gibi kapsüller (tünelleme). Sunucudan gelen paketleri de yerel alan ağına gönderir. Bu gönderme işleminden önce paketteki, sunucu tarafından eklenmiş kapsülü atar. Bütün bu alma ve gönderme işlerini Windows işletim sistemi TCP/IP yığınını (stack) kullanmadan, WinPcap [6] açık kaynak kodlu kütüphanesini kullanarak yapar.

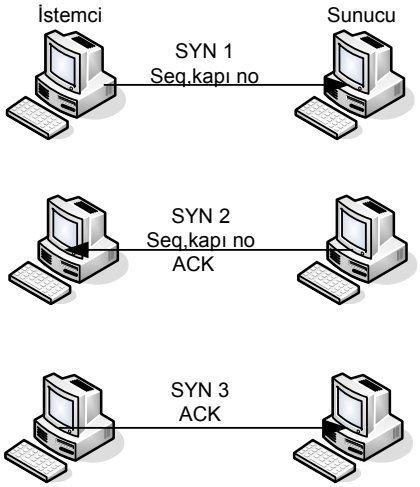


Şekil 2 Eklenen Başlıklar

İstemciye; sunucu ve istemci IP ve MAC adresleri ile yerel alan ağı, ağ geçidi MAC adresi önceden girilir.

İstemci temel olarak üç kısımdan oluşmuştur: Bağlantı kurma modülü, kapsülleme/kapsül atma ve gönderme modülü, koklayıcı (sniffer) modülü.

Bağlantı kurma modülü:
İstemci, Delphi 7.0 altında bulunan "Indy TCP Client"[7] kullanarak TCP 80 numaralı sunucu kapısına bağlanır. Bağlantı Şekil 3'deki gibi, TCP 3-yollu elsıkışma yoluyla gerçekleşir. İçerden dışarıya doğru yapılan bu bağlantı esnasında ateşduvarı, kaynak IP adresi ve kaynak kapı, hedef IP adresi ve hedef kapı numaralarını kaydeder. Daha sonra dışardan gelen paketlerde bu IP adresi ve kapı numaralarını kontrol eder, kaydedilen değerlerle aynı ise paketlerin geçişine izin verir [8].



Şekil 3 Bağlantı Kurulması (TCP 3-way handshake) [9]

İstemci kapısı da önemlidir. Statik olarak ayarlanan bu kapı adresi bazı anti-virüs/ateşduvarı yazılımları tarafından değiştirilebilmektedir. Bağlantı kurulması sırasında koklayıcı istemci kaynak kapı numarasını alır ve kapsüllleme/kapsül atma ve gönderme modülüne bildirir. Bağlantı kurulduktan sonra bağlantı kurma modülünün görevi biter. Şekil 3'de bağlantı kurma esnasında değişilen paketler görülmektedir.

SYN 1 paketi içinde istemci, sunucuya 0 – ($2^{\wedge 32}$-1) aralığında bir sayı bildirir (SEQ). SYN 2 paketinde sunucu, istemci tarafından gönderilen SEQ sayısını öğrendiğini ACK sayısı ile ve kendi SEQ sayısını bildirir. Son olarakta istemci, sunucunun SEQ sayısını öğrendiğini bildirir ve bağlantı kurulmuş olur. Bu bağlantı kurma işlemi, istemcide bulunan "Indy TCP Client" ve sunucuda bulunan "Indy TCP Server" modülleri tarafından Windows işletim sistemi TCP/IP yığını kullanılarak yapılır [7]. Koklayıcı modülü bu paketlerin değişimi esnasında SEQ numaralarını ve istemci TCP kapı numarasını öğrenerek kapsülleme/kapsül atma ve gönderme modülüne bildirir.

Kapsülleme\kapsül atma ve gönderme modülü:
Bağlantı kurma modülü, bağlantının kurulduğunu bildirmesinin ardından bu modül koklayıcı modülünden aldığı paketleri inceleyerek gerekli kapsülleme/kapsül atma ve gönderme işlerini yapar.

İstemci yazılımını ilgilendiren paketler, ya yerel alan ağı üzerindeki bilgisayarların birinden ya da internet üzerinden sunucudan gelir.

Yerel alan ağından gelen paketlerin hedef IP adresi, sunucu IP adresi (sunucuya verilen ikinci IP adresi. Şekil 4'te 192.168.0.14) ise veya paketin Ethernet hedef adresi FF:FF:FF:FF:FF:FF (yayım) ise, istemci yazılımı bu pakete Tablo 1'deki gibi sırasıyla TCP (HTTP), IP ve Ethernet başlıklarını ekler. İstemci yazılımı bu şekilde veriyi kapsülledikten sonra yerel alan ağına gönderir. Bu paketi yerel alan ağı, ağ geçidi alarak internet üzerinden sunucuya gönderir. Ağ geçidine gelmeden önce bu paket ateşduvarına gelir. (Ağ geçidi ateşduvarı da olabilir) Ateşduvarı paketteki kaynak ve hedef IP adresleri arasında daha önceden bir bağlantı kurulduğunu görür ve SEQ numarası da doğru olduğu için paketin geçmesine izin verir.

Şekil 4'te yerel alan ağından alınan paketlerin kapsülleme yapıldıktan sonra sunucuya gönderilişi gösterilmektedir.

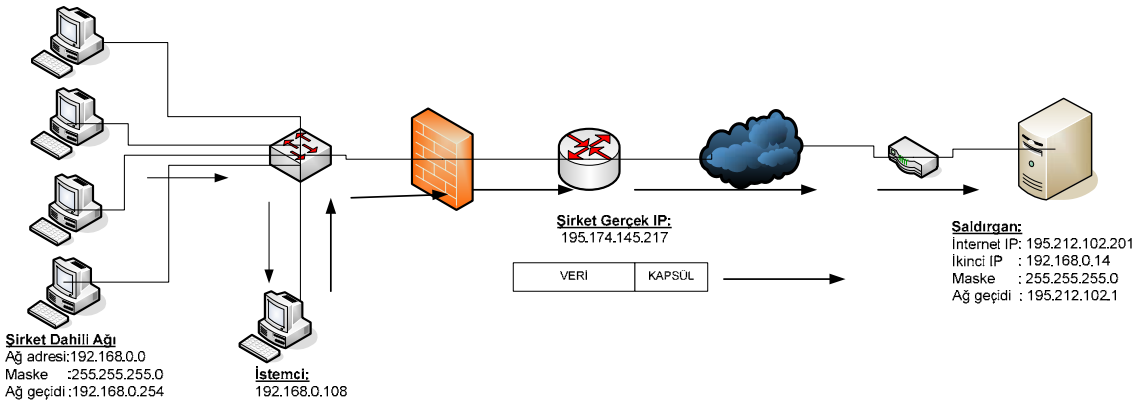
İstemci yazılımını ilgilendiren diğer paketler, internet üzerinden gelen sunucu bilgisayarın (saldırgan) gönderdiği paketlerdir. Bu paketlerin kaynak IP adresi sunucu bilgisayarın birinci IP adresidir (sunucu bilgisayarın internete çıkmak için kulladığı IP adresi, Şekil 5'te 195.212.102.201). İstemci bu paketleri alır, sunucu yazılımının eklediği kapsülü atar, kalan veri kısmını olduğu gibi yerel alan ağına gönderir. Bu paket doğrudan doğruya sunucu bilgisayarın adreslediği yerel alan ağı bilgisayarına gidecektir.

Şekil 5'te sunucu bilgisayardan gelen paketlerin kapsül atma işlemi yapıldıktan sonra yerel alan ağına gönderilişi gösterilmektedir.

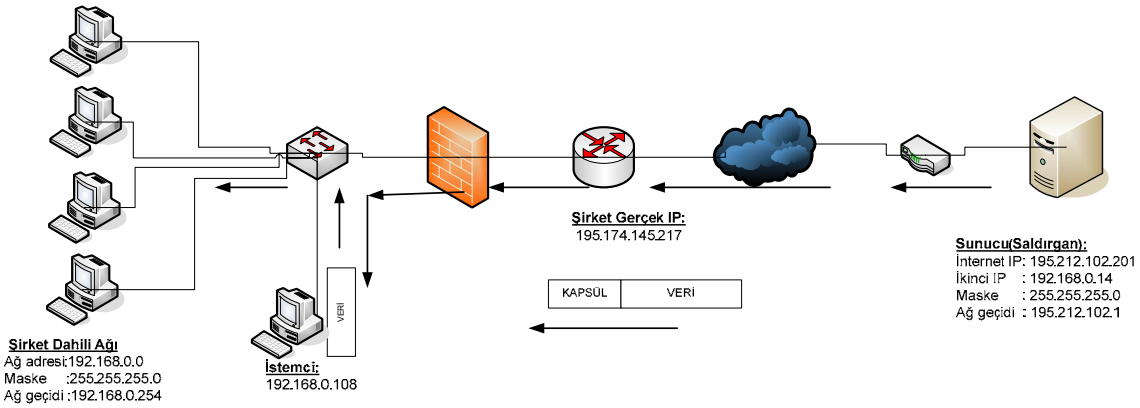
Kapsülleme/kapsül atma ve gönderme modülünün en önemli işlerinden bir tanesi de parçalama ve birleştirmedir. Ethernet yerel alan ağlarında default paket sekizli ikil (byte) miktarı 1500'dür [9]. Yerel alan ağından gelen paketteki sekizli ikil miktarı 1460'ı geçtiği zaman, bizim ekleyeceğimiz başlık kısmıyla birlikte 1500 sekizli ikili geçeceği için istemci yazılımı parçalama yapar. Sunucudan gelen pakette, eğer parçalanmış işareti varsa bu paketi saklar ve sonraki paketle birleştirdikten sonra yerel alan ağına gönderir.

ETHERNET	
Ethernet hedef adresi (MAC)	Yerel alan ağında kullanılan ağ geçidi MAC adresi.
Ethernet kaynak adresi (MAC)	İstemci yazılımın çalıştığı bilgisayarın MAC adresi
Ethernet Protocol	0x0800 Üst katman protokolünün IP olduğunu gösterir
IP	
IP version and length	0x45
IP service	0
IP length	40 + yakalanan paket uzunluğu
IP ident	X (rastgele bir sayı)+ 1 (her gönderilen pakette değeri 1 artırılır)
IP flags + offset	0x4000
IP time to live	0x80
IP protocol	0x06 Üst seviye protokolünün TCP olduğunu gösterir
IP checksum	Yönlendiriciler bu alanı kontrol eder, yanlışsa paketi göndermez. Bu alan hesaplanarak doğru değer yazılır.
Kaynak IP adresi	İstemci IP adresi
Hedef IP adresi	Sunucu birinci (internet) IP adresi
TCP	
TCP kaynak kapısı	Koklayıcı tarafından bağlantı kurulması esnasında yakalanır.
TCP hedef kapısı	0x5000
TCP sequence sayısı	Next sequence no= sequence no + bir önceki paketin uzunluğu
TCP ACK sayısı	ACK sayısı = en son sunucudan alınan paketin sequence sayısı + en son alınan paketin uzunluğu-54
TCP length,resv,flags	0x5018
TCP window	İstemcide ve sunucuda bu alan amacının dışında parçalama olup olmadığını kontrol için kullanılır.
TCP checksum	0x06d8 kontrol edilmediği için sabit değer girildi.
TCP urgent pointer	0

Tablo 1 İstemci tarafından Ethernet, IP ve TCP başlık alanlarına yazılan değerler.



Şekil 4 Yerel alan ağından alınan paketin sunucuya gönderilmesi



Şekil 5 Sunucudan gelen paketin yerel alan ağına gönderilmesi

Koklayıcı (Sniffer) Modülü:
Koklayıcı istemciye gelen tüm paketleri alır ve bu paketleri işlenmek üzere kapsülleme/kapsül atma ve gönderme modülüne gönderir. Bağlantı kurulması esnasında SEQ sayısı ve istemci TCP kapı değerini yakalar ve yine bunları kapsülleme/kapsül atma ve gönderme modülüne bildirir.

Bu modül ayrı bir iplik (thread) olarak ve olabildiğince hızlı çalışacak şekilde tasarlanmıştır.

4.1.2. Sunucu yazılımı

Sunucu yazılımı yerel alan ağındaki istemcinin internet üzerinden bağlandığı bir bilgisayar üzerinde çalışır. Bu bilgisayarın TCP 80 numaralı kapısına erişilir olmalıdır. İnternetle bağlantısını Ethernet protokolünü kullanarak yapıyor olmalıdır. Bu bilgisayar dial-up (çevirmeli ağ) olamaz, ADSL veya kablo internet bağlantısı olabilir. Sunucu yerel alan ağını Windows işletim sistemi ağ komşularımı kullanarak gösterir. Bunu sağlamak için Windows işletim sisteminin kendi TCP/IP yığınından yararlanılır. Daha önce anlatıldığı gibi Windows işletim sistemi bir bilgisayara birden fazla IP adresi verilmesine izin verir. Sunucu bilgisayarına ikinci IP adresi olarak, bağlantı yapılacak yerel alan ağı, ağ adresi aralığında ve o ağda kullanılmayan bir IP adresi verilir. Sunucu bilgisayarı yerel alan ağının bir parçası haline geleceği için IP adresi çakışması olmamalıdır. Diğer bilgisayarlardan gelen paketleri alabilmesi için de ikinci IP adresinin ağ adresi kısmı yerel alan ağı özel ağ adresi ile aynı olmalıdır. (Örn: 192.168.0.0)

Sunucu yazılımına, istemci ve sunucu IP (istemci IP adresi; yerel alan ağının internete çıkmak için kullandığı IP adresidir) ve MAC adresleri ile sunucu ağ geçidi MAC adresi önceden girilir.

Sunucu yazılımı da istemcide olduğu gibi üç parçadan oluşur: HTTP sunucu modülü, kapsülleme/kapsül atma ve gönderme modülü, koklayıcı modülü.

HTTP sunucu modülü:
Delphi 7.0 altında bulunan “Indy TCP Server”[7] modülü kullanılarak yazılmıştır. TCP 80 (HTTP) numaralı kapıyı dinler ve bu kapıya gelen bağlantı isteğini kabul eder. TCP bağlantısını başlatır. Bağlantı kurulduktan sonra bu modülün görevi biter. Kapsülleme/kapsül atma ve gönderme modülü devreye girer.

Kapsülleme\kapsül atma ve gönderme modülü:
HTTP sunucu modülü bağlantının kurulduğunu bildirmesinin ardından, bu modül koklayıcı

modülünden aldığı paketleri inceleyerek gerekli kapsülleme/kapsül atma ve gönderme işlerini yapar.

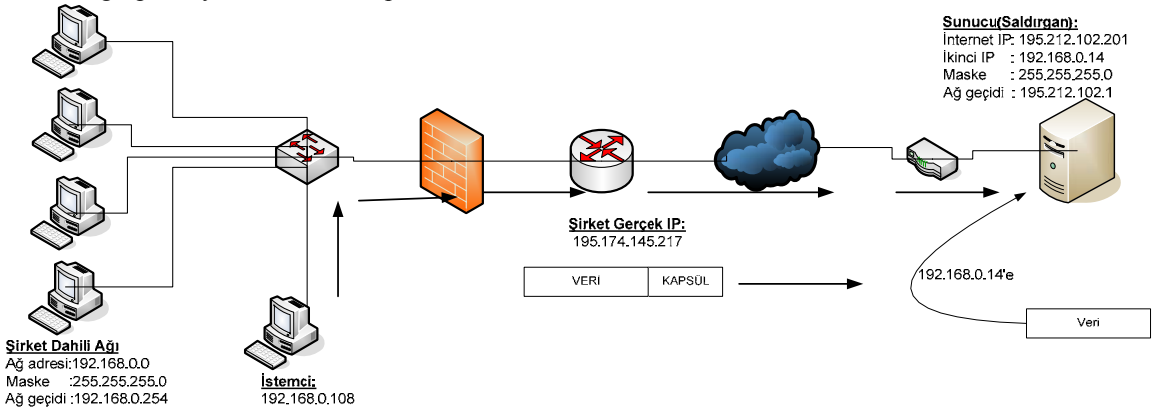
Sunucu yazılımını ilgilendiren paketler ya internet üzerinden, istemciden gelen paketler ya da sunucu bilgisayarının kendisinin yerel alan ağına göndermek istediği paketlerdir.

Kapsülleme/kapsül atma ve gönderme modülüne gelen paketlerin, kaynak IP adresi istemci bilgisayarının IP adresi ise (bu IP adresi yerel alan ağındaki tüm bilgisayarların kulandığı ortak internet IP adresidir), sunucu istemci tarafından eklenen kapsülü (Ethernet, IP ve TCP başlıkları) atar, geriye kalan veri kısmını kendi Ethernet kartından tekrar gönderir. Yerel alan ağından gelen bu paketin (kapsül atıldıktan sonra kalan paket) hedef IP adresi, sunucu Ethernet kartının ya ikinci IP adresi ya da yayımdır. Kendisinin gönderdiği ve yine kendisinin ikinci IP adresine (yerel alan ağ adresi) adresli paketi alan sunucu bilgisayarındaki Windows işletim sistemi, sunucu bilgisayarı yerel alan ağına bağlıymış gibi bu paketi işler. Örneğin bu paket Ping paketiyse buna cevap verir. Ana tarayıcıya (browser) yapılan bir sorgulamanın cevabı ise bunu yerel alan ağı komşularımda gösterir.

Şekil 6'de istemciden gelen bir paketin kapsülü atıldıktan sonra, sunucu paketi Ethernet kartından tekrar göndermekte ve ikinci IP adresi (192.168.0.14) tarafından alınmaktadır.

Eğer bir paketin hedef IP adresi yerel alan ağındaki bir bilgisayarın IP adresi ise ya da yayım ise (yalnızca kendisine ait yayımları) sunucu yazılımı bu paketleri aldığında Tablo 2'de açıklanan Ethernet, TCP ve IP başlıklarını ekler. (Eksik alanlar Tabo 1'deki gibi doldurulur)

İstemci de olduğu gibi kapsülleme/kapsül atma ve gönderme modülünün en önemli işlerinden bir tanesi de parçalama ve birleştirmedir. İstemciden gelen pakette eğer parçalama işaretlenmişse bu paketi saklar ve sonra gelen paketle birleştirdikten sonra gönderir.



Şekil 6 İstemciden gelen paketin sunucunun ikinci IP adresine gönderilmesi

ETHERNET	
Ethernet hedef adresi (MAC)	Sunucunun ağ geçidi MAC adresi.
Ethernet kaynak adresi (MAC)	Sunucu yazılımın çalıştığı bilgisayarın MAC adresi
IP	
Kaynak IP adresi	Sunucu birinci IP adresi (İnternet IP adresi)
Hedef IP adresi	İstemci IP adresi (İstemci yerel alan ağının internet IP adresi)
TCP	
TCP kaynak kapısı	0x5000
TCP hedef kapısı	Koklayıcı tarafından bağlantı kurulması esnasında yakalanır.

Tablo 2 Sunucu tarafından Ethernet, IP ve TCP başlık alanlarına yazılan değerler. Olmayan alanlar Tablo 1'deki gibi doldurulur.

Koklayıcı (Sniffer) Modülü:
İstemcide olduğu gibi çalışır.

4.2. Önemli İpuçları

1- İstemci yazılımı paket gönderme işlemine başlamadan, sunucuyla TCP 80 (HTTP) kapısı üzerinden bağlantı kurmaktadır. Bir yerel alan ağında bağlantıya her zaman açık olan kapı TCP 80 numaralı kapıdır. TCP 80 numaralı kapının açık olduğundan emin olduğumuz için bu kapı üzerinden sunucuya bağlanmakta sorun çıkmaz.

2- Windows işletim sistemi kendi TCP/IP yığınının haberi olmadan bir TCP/IP bağlantısına izin vermemektedir. Yani TCP istemci olarak bir sunucuyla bağlantı başlatılırsa, Windows işletim sistemi TCP/IP yığını sunucuya reset göndererek bu bağlantıyı sonlandırmaktadır. Bu sorunu aşmak için ilk bağlantı Windows işletim sistemi TCP/IP yığını kullanılarak yapıldı. Bunun için "Indy TCP server" ve "Indy TCP client" [7] modülleri kullanıldı. Bizim koklayıcımız da bu bağlantı esnasında gönderilip alınan SEQ numaralarını yakaladı. Bu SEQ numaraları daha sonra gönderilen paketlerde kullanılarak ateşduvarının paketlerimizi bloklamasının önüne geçildi.

   Ateşduvarı yerel alan ağından internete yapılan tüm bağlantıların kaydını tutar ve internetten gelen cevapların içerden yapılan bir bağlantının karşılığı olup olmadığını kontrol eder.

3- İstemcinin kendisine gelen tüm yayımları ve sunucuya adreslenmiş paketleri alarak bunları sunucuya gönderdiği 4.1.1'de anlatılmıştı. Yayımlar istemciye gelir fakat; sunucuya adreslenmiş bir paket nasıl olurda istemciye gelir? Sunucuya adreslenmiş bir paketin IP ve MAC adresi sunucuya ait olacaktır. Bu önemli bir sorun olmasına karşın sorunun çözümü için bir şey yapmamıza gerek yok; şöyleki istemci sunucudan gelen paketleri yerel alan ağına gönderirken bu paketlerin MAC adresi kısmında sunucunun MAC adresi olacaktır. Sunucu, yerel alan ağ anahtarına istemcinin bağlı olduğu ağ anahtarı kapısından (switch port) bağlanmış olur. Ağ anahtarı, sunucunun MAC adresiyle, paketin geldiği, yani istemcinin bağlı olduğu kapıyı (switch port) eşleştirir. Yerel alan ağından sunucunun MAC adresine gönderilen tüm paketler ağ anahtarı tarafından istemcinin bağlı olduğu kapıya (switch port) gönderilir. Burda hedef IP adresinin bir önemi yoktur çünkü; ağ anahtarı yalnızca MAC adreslerine bakarak paketi anahtarlar.

4- Ethernet yerel alan ağlarında bir paketin maksimum uzunluğu 1500 sekizli ikil olabilir. İstemcinin eklediği 20 sekizli ikil IP ve ayrıca 20 sekizli ikillik TCP başlığı fazladan eklendiği için, 1460 sekizli ikilden daha uzun paketler ağ anahtarı tarafından iletilmeyecektir. Bu nedenle istemci/sunucu yazılımları kapsülleme yapmadan önce paket uzunluklarını kontrol eder. 1460 sekizli ikilden daha uzun paketleri 2 parça halinde gönderir.

4.3. Örnek Uygulama Açıklaması

Bütün bu anlatılanların daha iyi anlaşılabilmesi için Ping uygulamasının nasıl çalıştığı aşağıda açıklanmıştır.

Şekil 4'deki yerel alan ağına bağlı 192.168.0.10 IP adresli bir bilgisayar "ping 192.168.0.14" komutunu komut satırından yazarak, sunucu ikinci IP adresini (yerel alan ağ IP adresi) pinglesin. Yerel alan ağına bağlı 192.168.0.14 IP adresli bir bilgisayar bulunmamaktadır. 192.168.0.10 IP adresli bilgisayar bu paketin kendi yerel alan ağında olması gereken bir bilgisayar olduğunu düşündüğünden, bu bilgisayarın MAC adresini öğrenmek için ARP paketi gönderir. ARP paketinin hedef MAC adresi FF:FF:FF:FF:FF:FF'tir yani yayımdır. İstemci bilgisayarımız bu yayımı alır ve daha önce anlattığımız gibi bu yayım paketini kapsüller. Kapsüllenen paketi tekrar yerel alan ağına gönderir. Bu defa paketi ağ geçidi alır ve kapsüldeki hedef IP adresi olan 195.202.102.1 adresine (sunucu internet IP adresi) gönderir.

Sunucu bilgisayarı bu paketi aldığında paketin kaynak IP adresine bakarak istemciden geldiğini anlar ve paketteki kapsülü atar. Kapsülü paketten attıktan sonra Şekil 6'deki gibi paketi kendi Ethernet kartından kendine tekrar gönderir. Bu bir yayım paketi olduğu için sunucunun hem birinci hem de ikinci IP adresleri bu paketi alır ve inceler. Bu paket ARP paketi olduğundan ve 192.168.0.14 IP adresinin MAC adresini sorduğu için 192.168.0.14 bir cevap ARP paketi hazırlar. Bu cevap ARP paketinin hedef IP adresi 192.168.0.10'dur. Daha önce anlatıldığı gibi sunucu yazılımı bu paketi alıp kapsülleme işlemini yaptıktan sonra internet üzerinden yerel alan ağına gönderir. Yerel alan ağına gelen paketin hedef kapı numarası istemci kapı numarası olduğu için yerel alan ağı yönlendiricisi paketi istemciye gönderir. İstemci paketteki kapsülü atar ve Şekil 5'deki gibi tekrar yerel alan ağına gönderir. Bu paket bir cevap ARP paketidir, hedef adresi 192.168.0.10'dur. 192.168.0.10 bilgisayarı bu paketi aldığında 192.168.0.14 bilgisayarının MAC adresini öğrenmiş olur. Bundan sonra hedef IP adresi 192.168.0.14 olan ping paketleri hazırlayarak yerel alan ağına gönderir.

Bu paketler 4.2 madde 3'de anlatılan sebepten dolayı istemci bilgisayarına gelir. Paketin hedef IP adresi sunucu ikinci IP adresi (yerel alan IP adresi) olduğu için istemci kapsülleme yaparak paketi sunucuya gönderir. Sunucu da daha önce anlatılan işlemler tekrar eder ve sonuçta ping cevap paketi 192.168.0.10 IP adresli bilgisayara ulaşır.

4.4. Testler

Testler ateşduvarı olmayan ve ateşduvarı olan yerel alan ağlarında ayrı ayrı yapıldı. Ateşduvarı olmayan

yerel alan ağlarında istemci ve sunucumuz başarıyla çalıştı. Ateşduvarı olan yerel alan ağlarında ateşduvarının özelliğine göre bazı durumlarda istemcimizin gönderdiği paketler bloklandı. Ateşduvarı eğer yalnızca durum takibi yapıyorsa (stateful inspection) istemcimiz çalıştı. Uygulama incelemesi (aplication or protocol inspection) yapan ateşduvarları istemcimizin gönderdiği paketleri blokladı ve sonuç olarak istemci çalışmadı. Anti-virüs programları istemciyi bir virüs olarak görmedi, istemcinin gönderdiği paketleri kötü niyetli bir aktivite olarak algılamadılar.

5. Sonuç

Bir istemci ve sunucu yazılımı yaparak, yerel alan ağlarının, sistem yöneticilerinin haberi olmadan internet üzerindeki bir bilgisayara nasıl bağlanacağını gösterdik. Saldırı içerden, şirket yerel alan ağına bağlı bir bilgisayar üzerinde bulunan, istemcinin çalıştırılarak saldırgana (sunucu) bağlanmasıyla başladı. Bu bir iç tehdittir. Şirket alan ağını koruyan ateşduvarları, sızma tespit ve önleme sistemleri bu saldırıyı engelleyemedi.

Yerel alan ağına bağlı saldırgan artık çeşitli saldırı tekniklerini kullanarak bu ağ üzerindeki şirket bilgilerini ve şifreleri kolaylıkla öğrenecektir.

Yerel alan ağlarını saldırılardan korumak için geliştirilen ateşduvarları, anti-virüs yazılımları, saldırı tespit ve önleme sistemleri dışardan gelecek saldırılar içindir, iç tehditler için sağladıkları önlemler sınırlıdır. Sistem yöneticileri ve ağ güvenlik sorumluları da iç tehditleri yeteri kadar bilmemekte ve önem vermemektedir. Dış tehditlere verilen önem kadar içten gelecek saldırılar için de sistemler ve yazılımlar geliştirilmeli, bu konuya daha fazla önem verilmelidir.

KAYNAKLAR

[1] Securing Cisco IOS Networks, Version 1.1, Cisco Systems, 2004

[2] D. Cappelli, A. Moore, R. Trzeciak, T.J. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition – Version 3.1, January 2009

[3] Frank L. Greitzer, Andrew P. Moore and Down M. Cappelli, Dee H. Andrews, Lynn A. Carroll, Thomas D. Hull, Comabating the Internal Cyberthreat, IEEE, Security and Privacy 2008, January/Ferbuary

[4] Ender Yüksel, Bülent Örencik, Sanal Özel Ağ Tasarımı ve Gerçeklemesi, EMO 1. Ağ ve Bilgi Güvenliği Sempozyumu, 2005

[5] Description of the Microsoft Computer Browser Service, Article ID:188001 Rev:3.2

[6] Politecnico di Torino, http://winpcap.polito.it

[7] www.indyproject.org

[8] Saadat Malik, Network Security Principles and Practices, Cisco Systems, 2003

[9] W.Richard Stevens, TCP/IP Illustrated, Volume1, Addison Wesley, 2001.