İçindekiler

[1. Hacker Araçları ve Savunmaların Yeni Cinsi 2](#_Toc10010036)

[2. Dağıtılmış Saldırılar 2](#_Toc10010037)

[2.1. Dağıtılmış Hizmet Reddi Saldırıları 3](#_Toc10010038)

[2.2. Dağıtılmış Hizmet Reddi Saldırılarına Karşı Savunma 4](#_Toc10010039)

[2.3. Dağıtılmış Şifre Kırma 4](#_Toc10010040)

[2.4. Dağıtılmış Parola Kırmaya Karşı Savunmalar 5](#_Toc10010041)

[2.5. Dağıtılmış Port Taraması 6](#_Toc10010042)

[2.5. Dağıtılmış Port Taramasına Karşı Savunma 7](#_Toc10010043)

[3. Röle Saldırıları 8](#_Toc10010044)

[4. Röle Saldırılarına Karşı Savunma 8](#_Toc10010045)

[5. Aktif Snifing 8](#_Toc10010046)

[5.1. Geleneksel Snifﬁng 9](#_Toc10010047)

[5.2. Aktif Snifing ile Antenin Yükseltilmesi 9](#_Toc10010048)

[5.3. MAC Adreslerinin Taşması 9](#_Toc10010049)

[5.4. Sahte ARP Trafiği 10](#_Toc10010050)

[5.5. Sahte DNS İstemcisi 11](#_Toc10010051)

[5.6. SSL Saldırısı 12](#_Toc10010052)

[5.7. Aktif Snifing Tekniklerine Karşı Savunma 12](#_Toc10010053)

[6. Social Engineering: The Forgotten Risk - Sosyal Mühendislik: Unutulmuş Risk 14](#_Toc10010054)

[7. Sosyal Mühendisliğin Tanımlanması 14](#_Toc10010055)

[8. Sosyal Mühendislik Neden İş Yapıyor? 14](#_Toc10010056)

[8.1.İnsan Doğası 14](#_Toc10010057)

[8.2.İş Ortamı 16](#_Toc10010058)

[8.3. İstihparat Toplama 16](#_Toc10010059)

[8.4. Hedef Seçme 16](#_Toc10010060)

[8.5. Saldırı 17](#_Toc10010061)

[8.5.1. Ego Attacks 17](#_Toc10010062)

[8.5.2. Sempati Atakları 17](#_Toc10010063)

[8.5.3. Sindirme Saldırıları 17](#_Toc10010064)

[9. Riski Azaltma 17](#_Toc10010065)

# 1. Hacker Araçları ve Savunmaların Yeni Cinsi

Ed Skoudis, CISSP

Bilgisayar saldırı araç ve tekniklerinde son teknoloji hızla ilerlemektedir. Evet, hizmet reddi saldırıları, şifre kırıcılar, port tarayıcılar, sniffers ve RootKits gibi geleneksel bilgisayar saldırısı araçlarının on yıllardır süren gerçek cephaneliğiyle karşı karşıyayız. Bununla birlikte, bu temel araç ve tekniklerin birçoğu son birkaç yıl içinde, onları her zamankinden daha güçlü kılan yeni özellikleri ve temel mimarileri ile bir rönesans gördü. Saldırganlar yaygın olarak kullanılan protokollere ve işletim sistemimizin kalbine derinlemesine giriyorlar. Büyüyen yeteneklerine ek olarak, bilgisayar saldırı araçlarının kullanımı giderek daha kolay hale geliyor. Her şeyi gördüğünüzü düşündüğünüzde, çoraplarınızı patlatan bir özellik ile yeni ve kullanımı kolay bir saldırı aracı kullanıma sunuldu. Gelişmişliği ve saldırı araçlarında kullanım kolaylığındaki bu sürekli artış ve zayıf hedeflerin internete yaygın biçimde yayılmasıyla birlikte, şimdi hacklemenin altın çağında yaşıyoruz. Bu bölümün amacı, bilgisayar saldırı araçlarının bu evrimindeki son olayları tanımlamaktır. Bilgisayarlarımız için en iyi savunmayı oluşturmak için kişinin rakiplerinin yeteneklerini ve taktiklerini anlamak gerekir. Bu amaca ulaşmak için, bu bölüm, her bir saldırı türü için savunma teknikleriyle birlikte, dağıtılmış saldırılar, aktif tarama ve çekirdek seviyesi RootKits dahil olmak üzere saldırı araçları arasında birkaç ilerleme alanı açıklamaktadır.

# 2. Dağıtılmış Saldırılar

Bilgisayar saldırı araçlarının evrimindeki ana eğilimlerden biri, dağıtılmış saldırı mimarilerine doğru hareketidir. Esasen, saldırganlar saldırı yeteneklerini geliştirmek için İnternet'in dağıtılmış gücünü kullanıyor. Buradaki strateji oldukça basit, belki de aldatıcı bir biçimde bu dağıtılmış saldırı araçlarının bazılarının gücü göz önüne alındığında. Saldırgan, geleneksel bir bilgisayar saldırısı alır ve işi birçok sistem arasında böler. Saldırıda giderek daha fazla sistemle birlikte saldırganın başarı şansı artıyor. Bu dağıtılmış saldırılar, saldırganlara aşağıdakiler dahil birçok avantaj sunar:

• Tespit edilmeleri daha zor olabilir.

• Saldırganın izini sürmek için genellikle işleri daha zorlaştırırlar.

• Saldırıyı hızlandırabilir ve belirli bir sonuca ulaşmak için gereken zamanı azaltabilirler.

• Bir saldırganın bir hedefte daha fazla kaynak tüketmesine izin verir.

Öyleyse, saldırgan tüm makinelerin dağıtılmış bir saldırı başlatmasını nereden sağlıyor? Ne yazık ki, İnternet'te çok sayıda çok zayıf makine bulunmaktadır. Bu tür sistemlerin yöneticileri ve sahipleri, satıcılardan güvenlik yamaları uygulamazlar ve makinelerini güvenli bir şekilde yapılandırmazlar, çoğu zaman yalnızca kutudan çıktığı varsayılan konfigürasyonu kullanırlar. Üniversitelerdeki kötü güvenlikli bilgisayarlar, her büyüklükteki şirketler, devlet kurumları, sürekli İnternet bağlantısı olan evler ve başka yerlerdeki saldırganlar için kolay avlardır. Çok az yetenekli saldırganlar bile dünya çapında yüzlerce veya binlerce sistemi kolaylıkla alabilirler. Bu saldırganlar, Internet’in büyük alanlarını taramak için ev yapımı komut dosyaları ve Nessus güvenlik açığı tarayıcısı (http://www.nessus.org) gibi ücretsiz araçlar da dahil olmak üzere otomatik güvenlik açığı tarama araçlarını kullanır.

Saldırganlar birçok klasik bilgisayar saldırı aracını dağınık bir paradigmaya uyarladılar. Bu bölüm, hizmet reddi saldırıları, dağıtılmış parola kırma, dağıtılmış bağlantı noktası taraması ve aktarma saldırıları da dahil olmak üzere en popüler dağıtılmış saldırı araçlarının çoğunu incelemektedir.

# 2.1. Dağıtılmış Hizmet Reddi Saldırıları

En popüler ve yaygın olarak kullanılan dağıtılmış saldırı tekniklerinden biri dağıtılmış hizmet reddi (DDoS) saldırısıdır. Bir DDoS saldırısında, saldırgan çok sayıda sistemi devralır ve her sisteme zombi denilen uzaktan kumandalı bir program yükler. Zombiler sessizce komutları bekleyen arka planda koşuyorlar. Saldırgan, bu zombi sistemlerini bir makinede çalışan özel bir istemci programı kullanarak kontrol eder. Saldırgan çok sayıda zombiye komut göndermek için bir istemci makinesi kullanıyor ve onlara aynı anda bazı eylemler yapmalarını söylüyor. Bir DDoS saldırısında en yaygın eylem, paketleri olan bir kurbanı öldürmektir. Tüm zombiler eşzamanlı olarak paket bataklıkları başlattığında, kurban makinesi aniden sahte trafikte yıkanacak. Mağdurun iletişim bağlantısının tüm kapasitesi tükendiğinde, meşru bir kullanıcı trafiği sisteme ulaşamaz ve bu da hizmet reddine neden olur. DDoS saldırı metodolojisi, Şubat 2000'de, yüksek düzeyli İnternet sitelerinin saldırıya maruz kaldığı gün ışığı altındaydı. DDoS araçları daha da ıslatan yeni özelliklerle gelişmeye devam etti. En yeni nesil DDoS saldırıları, geniş kapsamlı göz atma yetenekleri içeriyor, böylece müşteriden zombilere ve zombilerden hedefe giden tüm trafik tuzak kaynağı bir adrese sahip. Bu nedenle, bir proje başladığında, araştırmacılar, saldırgandan zombilere, saldırganın yönlendirici sıçramasıyla saldırganın geçmişini izlemelidir. Bazı zombileri topladıktan sonra, araştırmacılar hala zombilerden müşteriye, sayısız atlama noktasına ve birden fazla İnternet servis sağlayıcısına (İSS'ler) devam etmelidir. Ayrıca, DDoS araçları zombilerin yerini gizlemek için şifreleme kullanıyor. İlk nesil DDoS araçlarında, istemci yazılımının çoğu, zombiler için bir ağ adresleri listesi içeren bir dosya içeriyordu. Böyle bir müşteriyi keşfederek, bir soruşturma ekibi zombileri hızla bulabilir ve ortadan kaldırabilir. En yeni nesil DDoS araçlarıyla, istemcideki ağ adreslerinin listesi güçlü bir şekilde şifrelenir, böylece müşteri zombilerin yerini vermez.

# 2.2. Dağıtılmış Hizmet Reddi Saldırılarına Karşı Savunma

DDoS saldırıları da dahil olmak üzere herhangi bir pakete karşı savunma yapmak için, kritik ağ bağlantılarının basit saldırıları ortadan kaldırmak için yeterli bant genişliğine ve fazlalığına sahip olması sağlanmalıdır. Eğer bir ağ bağlantısı kritikse, en azından yedekli bir T1 bağlantısı olmalıdır, çünkü tüm düşük bağlantı hızları bir saldırgan tarafından kolayca çözülebilir. Bu bant genişliği taban çizgisi en düşük saldırgan seviyelerini ortadan kaldırırken, kişi yüz veya bin sisteme zombi kuran ve sisteminize işaret eden saldırganlara yetişmek için yeterli bant genişliğini satın alamayacak olması gerçeğiyle yüz yüze gelmelidir.

Bir sistemin Internet’te kullanılabilir olması iş için kritik öneme sahipse, DDoS saldırılarını ele almak için ek teknikler kullanılması gerekir. Teknolojik açıdan bakıldığında, gelen oturumların sayısının yönetilmesine yardımcı olacak, böylece sunucularının ezilmemesi için trafik şekillendirme araçlarını düşünmek isteyebilir. Tabii ki, birinin bağlantısını kaldıran yeteri kadar büyük bir zombi kadrosu, trafiğin şekillendiricilerini bile ezebilir. Bu nedenle, bir saldırının ne zaman gerçekleşeceğini belirlemek için izinsiz giriş tespit sistemleri (IDS'ler) kullanılmalıdır. Bu IDS'ler, ağ hırsız alarmları gibi davranır, IDS veritabanında depolanan yaygın saldırı imzalarıyla eşleşen trafiği izler. Prosedürel bir bakış açısına göre, IDS'den gelen bu tür alarmlar için bekleme modunda bir olay müdahale ekibi bulunmalıdır. Görev açısından kritik İnternet bağlantıları için, birinin ISS’nin kendi olay müdahale ekibi için cep telefonu ve çağrı cihazı numaraları olması gerekir. Bir DDoS saldırısı başladığında, birinin olay müdahale ekibi, ISS’nin olay müdahale ekibinin kuvvetlerini hızlı ve etkili bir şekilde yakalayabilmelidir. Bir kez uyarı verildiğinde, ISS, aktif DDoS saldırılarını engellemek için ağlarına filtreler yerleştirebilir.

# 2.3. Dağıtılmış Şifre Kırma

Şifre kırma işleminin ardındaki fikir basit: şifreli bir şifre dosyası çalmak, bir şifre tahmin etmek, tahminde bulunmak ve sonucu çalınan şifreli dosyadaki değerle karşılaştırmak. Şifreli tahmin şifreli parola ile eşleşiyorsa, saldırgan parolayı belirlemiştir. İki değer eşleşmezse, saldırgan başka bir tahminde bulunur. Kullanıcı şifreleri genellikle kullanıcı kimlikleri, sözlük sözcükleri ve diğer karakterlerin tahmin edilebilir kombinasyonları olduğundan, bu teknik genellikle şifreleri belirlemede çok başarılıdır.

Geleneksel parola kırma araçları, parolaların hızlı ve verimli bir şekilde belirlenmesine yardımcı olmak için tahmin-şifreleme-karşılaştırma döngüsünü otomatikleştirir. Bu araçlar, kullanıcı kimliğinin varyasyonlarını, sözlük terimlerini ve şifreler için tahminlerini oluşturmak için olası tüm karakter kombinasyonlarının kaba kuvvet tahminini kullanır. Daha iyi şifre kırma araçları hibrit saldırılar yapabilir, karakterleri kaba bir şekilde standart sözlük kelimelerine ekleyebilir ve hazırlayabilir. Şifrelerin çoğu, başında veya sonunda basılan birkaç özel karakterden oluşan bir sözlük terimi olduğu için, karma teknik son derece kullanışlıdır. En iyi geleneksel şifre kırma araçlarından bazıları, Windows NT şifreleri için L0phtCrack (http://www.l0pht.com adresinde bulunur) ve UNIX ve Windows NT (http: / adresinde bulunabilir) de dahil olmak üzere çeşitli şifre türleri için Ripper John'dur. /www.openwall.com).

Daha kısa sürede daha fazla şifre tahminleri oluşturabilen ve kontrol edebilen araçlar, saldırganın kurtardığı daha fazla şifre ile sonuçlanacaktır. Geleneksel şifre kırma araçları, tahminleri şifrelemek için kullanılan şifreleme algoritmasının uygulanmasını optimize ederek bu hız sorununu giderir. Saldırganlar parola kırma yükünü çok sayıda bilgisayara dağıtarak daha da fazla hız kazanabilirler. Şifreleri daha hızlı bir şekilde kırmak için saldırganlar aynı anda şifreli bir şifreyle şifrelenmiş şifreleri çalmak için İnternet üzerinden yerleştirilmiş yüzlerce veya binlerce sistemi kullanacaklardır. Dağıtılmış şifre kırma uygulamak için, saldırgan, işi manuel olarak bölerek geleneksel bir şifre kırma aracını dağıtılmış bir şekilde kullanabilir. Örneğin, bir saldırganın, şifrelenmiş on şifreyle şifreli bir şifre kırmak istediği bir senaryo düşünün. Saldırgan, her biri şifreli bir şifre içeren, bölümü on parçaya bölebilir ve ardından her bir parçayı on makineden birine dağıtabilir. Her makine, söz konusu sisteme atanmış şifreli şifreyi kırmak için geleneksel bir şifre kırma aracı kullanır. Alternatif olarak, saldırgan makinelerin her birine şifrelenmiş on şifreyi yükleyebilir ve her bir geleneksel şifre kırma aracını, bir kaba kuvvet saldırısında bir sözlüğün veya belirli karakterlerin farklı bir kısmına odaklanarak farklı bir şifre kümesi tahmin etmesi için yapılandırabilir.

Çalışmayı el ile bölmenin ve geleneksel bir şifre kırma aracı kullanmanın ötesinde, birkaç yerel dağıtılmış şifre kırma aracı piyasaya sürüldü. Bu araçlar, iş yükünün birkaç makineye yayılmasını otomatikleştirmeye ve saldırı ilerledikçe bilgi işlem kaynaklarını koordine etmeye yardımcı olur. En popüler dağıtılmış parola kırma araçlarından ikisi Mio-Star ve Saltine Cracker, ikisi de http://packetstorm.securify.com/distributed adresinde bulunabilir.

# 2.4. Dağıtılmış Parola Kırmaya Karşı Savunmalar

Dağıtılmış parola kırmaya karşı savunmaları gerçekten geleneksel parola kırma için kullanılanlarla aynıdır: zayıf parolaları sisteminizden kaldırın. Dağıtılmış parola kırma işlemi, kırma işlemini hızlandırdığından, parolaların dağıtılmamış parola kırma işleminin hüküm sürdüğü günlerden daha zor olması gerekir. Kullanıcıları minimum uzunluktan daha büyük (dokuz karakterden daha büyük) şifreleri oluşturmaya zorlayan ve her bir şifreye rakam, harf ve özel karakterler içeren bir politika ile başlamalıdır. Kullanıcılar politikanın farkında olmalıdır; bu nedenle, tahmin edilebilecek şifrelerin önemini vurgulayan bir farkındalık programı anahtardır. Ayrıca, bir şifre politikasının uygulanmasına yardımcı olmak için, birinin kimlik doğrulama sunucularında şifre filtreleme araçları kullanmak isteyebilirsiniz. Bir kullanıcı yeni bir şifre belirlediğinde, bu araçlar şifre politikasına uygun olduğundan emin olmak için şifreyi kontrol eder. Şifre çok kısa ise veya rakam, harf ve özel karakter içermiyorsa, kullanıcıdan başka bir şifre seçmesi istenir. Windows NT Kaynak Seti'ndeki pass ﬁ lt.dll programı ve UNIX sistemlerindeki passwd + programı, bazı üçüncü taraf eklenti kimlik doğrulama ürünlerinde olduğu gibi bu özelliği uygular. Biri de, token tabanlı erişim teknolojilerini kullanarak standart şifrelerin çok hassas ortamlardan kaldırılmasını düşünmek isteyebilir.

Son olarak, güvenlik personeli, saldırganın yapmadan önce zayıf olanlarını belirlemek için periyodik olarak bir kullanıcının kendi parolalarına karşı bir şifre kırma aracı çalıştırmalıdır. Zayıf şifreler bulunduğunda, kullanıcıları daha iyi bir şifre seçmeleri gerektiği konusunda bilgilendirmek için belirlenmiş ve onaylanmış bir süreç olmalıdır. Yönetimin bu önemli güvenlik programını anlamasını ve desteklemesini sağlamak için kurum içi şifre kırma projeleri gerçekleştirmeden önce uygun izinleri aldığınızdan emin olun. Yönetim onayının alınmaması, birinin kariyerini olumsuz yönde etkileyebilir.

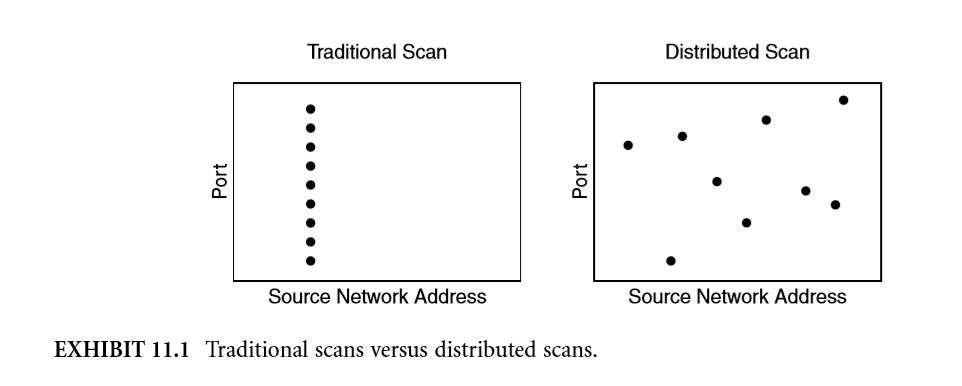
# 2.5. Dağıtılmış Port Taraması

Dağınık bir yaklaşıma kendini iyi veren bir başka saldırı tekniği de liman taraması. Bir bağlantı noktası, İnternet hizmetlerinin büyük çoğunluğu tarafından kullanılan iki iletişim kuralı olan İletim Denetimi Protokolünde (TCP) ve Kullanıcı Veri Birimi Protokolünde (UDP) önemli bir kavramdır. Bir ağdan TCP veya UDP trafiği alan her sunucu bir veya daha fazla bağlantı noktasını dinler. Bu bağlantı noktaları, paketlerin girip çıkabileceği bir makinedeki küçük sanal kapılar gibidir. Port numaraları, paketlerin yönlendirilmesi gereken bir sistemde adresler olarak hizmet eder. Bir yönetici bir ağ servisini herhangi bir porttan dinlemek için yapılandırabilirken, en yaygın servisler iyi bilinen portlardan dinler, böylece istemci yazılımı paketleri nereye göndereceğini bilir. Web sunucuları genellikle 80 numaralı TCP bağlantı noktasını dinlerken, İnternet posta sunucuları 25 numaralı TCP bağlantı noktasını dinler. Etki Alanı Adı Sunucuları, UDP bağlantı noktası 53'teki sorguları dinler. RFC 1700'deki http: / adresinde bulunan bir belge olan çeşitli hizmetlere yüzlerce başka bağlantı noktası atanmıştır. /www.ietf.org/rfc.html.

Port tarama, hangi portların dinleme servislerinin olduğunu belirlemek için hedef sistemdeki çeşitli portlara paket gönderme işlemidir. Hangisinin açık olduğunu görmek için hedef sistemin kapılarını çalmaya benzer. Saldırganın hedef sistemde hangi bağlantı noktalarının açık olduğunu bilmesiyle, makinede çalışan hizmetler hakkında iyi bir fikri vardır. Saldırgan daha sonra bu açık bağlantı noktalarıyla ilişkili hizmetlere bir saldırıya odaklanabilir. Ayrıca, hedef sistemdeki her bir açık bağlantı noktası, saldırgan için olası bir giriş noktasını belirtir. Saldırgan, makineyi tarayabilir ve TCP bağlantı noktası 25 ve UDP bağlantı noktası 53'ün açık olduğunu belirleyebilir. Bu sonuç, saldırgana makinenin muhtemelen bir posta sunucusu ve DNS sunucusu olduğunu söyler. Çok sayıda geleneksel portscanning aracı mevcut olsa da, en güçlülerinden biri (bugüne kadar) http://www.insecure.org adresinde bulunan Nmap aracıdır.

Bir port taraması genellikle daha derinlemesine bir saldırının öncüsü olduğundan, güvenlik personeli port taramalarını erken uyarı göstergesi olarak algılamak için genellikle IDS araçlarını kullanır. Çoğu IDS, port taramalarını tanımak için özel yetenekler içerir. Bir paket bir bağlantı noktasına giden belirli bir kaynaktan gelir, ardından aynı kaynaktan başka bir bağlantı noktasına giden başka bir paket takip eder, ardından başka bir bağlantı noktası için başka bir paket gelirse, IDS bu paketleri taramanın tespit edilmesi için hızlı bir şekilde ilişkilendirebilir. Bu trafik şekli, port numaralarının kaynak ağ adresine göre çizildiği, Ek 11.1'in sol tarafında gösterilmiştir. IDS'ler böyle bir taramayı kolayca tespit edebilir ve zil ve ıslık çalabilir (veya yöneticiye e-posta gönderebilir).

Şimdi bir saldırgan taramayı gerçekleştirmek için dağıtılmış bir yaklaşım kullandığında ne olacağını düşünün. Saldırgan, tek bir adresten gelen bir paket barajı yerine, taramaya katılmak için birçok sistemi yapılandırır. Her tarama makinesi yalnızca bir veya iki paket gönderir ve sonuçları alır. Birlikte çalışarak, tarama makineleri, hedef sistemdeki tüm ilginç portları kontrol edebilir ve sonuçlarını saldırgan tarafından ilişkilendirilmek üzere gönderebilir. Geleneksel port taramasının tanıdık şeklini arayan bir IDS saldırıyı tespit etmeyecektir. Bunun yerine, gelen paketlerin düzeni, Ek 11.1'in sağ tarafında gösterildiği gibi, daha rastgele görünecektir. Bu şekilde, dağıtılmış tarama, saldırıların tespitini daha zorlaştırır.



Elbette bir IDS sistemi, kaynak adres yerine hedef adrese (yani paketlerin gittiği yer) odaklanarak dağıtılmış bağlantı noktası taramasını algılayabilir. Birden fazla sistem birdenbire tek bir makinedeki birkaç bağlantı noktasına paketleri gönderirse, bir IDS bağlantı noktası taramasının devam ettiğini tespit edebilir. Ancak saldırgan, dağıtılmış bir tarama yaparak algılama için çıtayı yükseltmiştir. Dağıtılmış tarama daha uzun bir süre boyunca gerçekleştirilirse (örneğin, bir hafta veya ay), bir IDS'den kurtulma şansı bir saldırgan için oldukça iyidir. Dağıtılmış bağlantı noktası taramaları, bir saldırganın izini sürmek için çok daha zordur, çünkü tarama, hiçbiri saldırganın sahip olmadığı pek çok farklı sistemden gelir. Birkaç dağıtılmış bağlantı noktası tarama aracı mevcuttur.

Saldırgan, tarama yapmak için Web sunucularına yerleştirilebilecek küçük bir komut dosyası olan açıklayıcı olarak adlandırılan Phpdistributedportscanner'ı kullanabilir. Saldırganlar PHP etkin bir Web sunucusunu ele geçirdiklerinde, komut dosyasını sunucuya yerleştirebilir ve diğer sistemleri taramak için kullanabilirler. Saldırgan, HTTP isteklerini kullanarak çeşitli Web sunucularında çalışan ayrı tarama komut dosyaları ile etkileşime girer. Her şey Web tabanlı olduğundan, dağıtılmış bağlantı noktası taramalarının çalıştırılması oldukça basittir. Bu tarama aracı http://www.digitaloffense.net:8000/phpDistributedPortScanner/ adresinde bulunabilir. Diğer dağıtılmış bağlantı noktası tarayıcıları, Dscan (http://packetstorm.securify.com/distributed adresinde bulunabilir) ve SIDEN (http://siden.sourceforge.net adresinde bulunabilir) gibi bir istemci / sunucu mimarisine dayanma eğilimindedir.

# 2.5. Dağıtılmış Port Taramasına Karşı Savunma

Dağıtılmış bağlantı noktası taramasına karşı en iyi savunma, birinin sistemindeki tüm gereksiz hizmetleri kapatmaktır. Bir makinenin tek amacı, HTTP ve HTTPS ile iletişim kuran bir Web sunucusunu çalıştırmaksa, sistemin sadece 80 numaralı TCP portu ve 443 numaralı TCP portu açık olmalıdır. Bir web sunucusu ile aynı makinede çalışan bir posta sunucusuna ihtiyaç duymuyorsa, posta sunucusunun devre dışı bırakılması için sistem yapılandırılmalıdır. Makinede X Pencere sistemi gerekli değilse, kapatın. Diğer tüm servisler kapatılmalı, bu diğer bütün portları kapatacaktır. Bir kişi, güvenli sunucular oluşturmak için bir kuruluştaki tüm sistem yöneticileri için adım adım bir işlem sağlayan güvenli bir yapılandırma belgesi geliştirmelidir. Ek olarak, IDS problarının güncel tutulmasını sağlamalıdır. Çoğu IDS satıcısı düzenli olarak yeni saldırı imzaları dağıtır - genellikle ayda bir kez. Yeni bir saldırı imzası kümesi mevcut olduğunda, kişi hızlı bir şekilde test etmeli ve IDS problarına dağıtmalıdır, böylece en son saldırı kümesini tespit edebilsinler.

# 3. Röle Saldırıları

Son bir dağıtılmış saldırı tekniği, saldırının gerçek kaynağını gizlemek için bilgilerin makineden makineye İnternet üzerinden aktarılmasını içerir. Tahmin edilebileceği gibi, çoğu saldırgan yakalanmak istemiyor. Saldırgan ve hedef arasında fazladan dolaylı aktarım katmanları kurarak saldırgan yakalanmaktan kaçınabilir. Bir saldırganın tüm dünyada bulunan ve İnternet üzerinden erişilebilen yarım düzine makineyi alıp yeni bir sisteme saldırmak istediğini varsayalım. Saldırgan altı sistemde paket yönlendirici programları ayarlayabilir. İlk makine, belirli bir porttan alınan paketleri ikinci sisteme iletir. İkinci sistem daha sonra onları üçüncü sisteme yönlendirir ve böylece yeni hedefe ulaşılana kadar devam eder. Her sistem, saldırganın trafiği için bir röle zincirinde bir link görevi görür. Saldırı tespit edildiğinde ve tespit edildiğinde, soruşturma ekibinin, saldırganı bağlamadan önce her röle noktasından saldırıyı izlemesi gerekecektir.

Saldırganlar genellikle dünya genelinde çok sayıda sistemden oluşan röle zincirleri kurarlar. Ek olarak, diğer araştırmacılara da saldırganlar saldırganlar sık ​​sık röle zincirinin bağlantılarının bulunduğu ülkeler arasında insan dili ve jeopolitik ilişkilerde büyük bir değişiklik olduğundan emin olmaya çalışır. Örneğin, ilk röle Amerika Birleşik Devletleri'nde, ikincisi ise Çin'de olabilir. Üçüncüsü Hindistan’da olabilir, dördüncüsü Pakistan’da. Sonunda, zincir İran’da ABD’de bulunan bir makineye saldırı için son buluyor. Aktarma zincirinin her aşamasında, araştırmacıların insan dilindeki dramatik değişimler, ülkeler arasındaki dostluktan daha az ilişkiler ve devasa kanun uygulayıcı yargı meseleleriyle mücadele etmeleri gerekecekti. Röle saldırıları genellikle, http://www.l0pht.com/users/10pht/ nc110.tgz adresinde UNIX ve http: //www.l0pht adresindeki Windows NT için kullanılabilen Netcat adlı çok esnek bir araç kullanılarak gerçekleştirilir. com / ~ kaynak / netcat'in /. Röle oluşturmanın bir diğer popüler aracı ise http: // oh.verio.com/~sammy/hacks adresinde bulunur.

## 4. Röle Saldırılarına Karşı Savunma

Geçiş saldırılarındaki eylemlerin çoğu bir kuruluşun kendi ağının dışında gerçekleştiği için, bu tür saldırıları önlemek için yapılabilecek çok az şey var. Biri saldırıya uğramadan önce saldırganların paketlerini bir grup makineden geçirmesini engelleyemez. En iyi bahis, güvenlik yamaları uygulayarak ve tüm gereksiz hizmetleri kapatarak sistemlerin güvenli olduğundan emin olmaktır. Ek olarak, bu tür saldırılara ilişkin soruşturmalarda, yetkililerin yasaların uygulanması ile işbirliği yapılması önemlidir.

# 5. Aktif Snifing

Snifing, yeni yeteneklerle hızla genişleyen bir başka eski tekniktir. Geleneksel koklayıcılar bir ağdan trafik toplayan basit araçlardır. Kullanıcı, bilgisayara ya da başka bir sisteme yönelik olsun olmasın, bilgisayarın ağ arabiriminden geçen tüm verileri toplayan bir bilgisayara bir sniffer programı yükler. Ağ yöneticileri tarafından kullanıldığında, koklayıcılar ağın sorunlarını gidermeye yardımcı olmak için hatalı paketleri yakalayabilir. Saldırganlar tarafından kullanıldığında, sniffers, şifreler, dosyalar, e-postalar veya ağda iletilen herhangi bir şey gibi ağdan hassas verileri alabilir.

# 5.1. Geleneksel Snifﬁng

Geleneksel bıçaklama araçları pasiftir; trafiğin ağdan geçmesi ve geldiğinde verileri toplaması için sabırla beklerler. Bu pasif teknik bazı ağ tipleri için iyi çalışıyor. Çok sayıda yerel alan ağı (LAN) oluşturmak için kullanılan popüler bir teknoloji olan Geleneksel Ethernet, bir yayın ortamıdır. Ethernet hub'ları geleneksel Ethernet LAN'ları oluşturmak için kullanılan cihazlardır. LAN üzerindeki herhangi bir sisteme gönderilen tüm trafikler, LAN üzerindeki tüm makinelere yayınlanır. Geleneksel bir sniffer bu nedenle aynı LAN'daki diğer sistemler arasında giden herhangi bir veriyi yakalayabilir. Geleneksel bir saldırı saldırısında, saldırgan LAN'a bir sistem devraldı, bir sniffer taktı ve aynı LAN üzerindeki diğer makineler için tutulan trafiği topladı. En iyi geleneksel sniffer'lerden bazıları Snort (http://www.snort.org adresinde bulunur) ve Snif (t (http://reptile.rug.ac.be/~coder/snif ﬁ t / snif ﬁ t.html adresinde bulunur). Geleneksel sniffers'a karşı yaygın olarak kullanılan savunmalardan biri, anahtarlamalı bir LAN'dir.

Bir yayın aracı görevi gören bir Ethernet hub'ının aksine, Ethernet anahtarı yalnızca LAN üzerindeki amaçlanan hedefine veri gönderir. LAN üzerindeki başka hiçbir sistem verileri göremez, çünkü Ethernet anahtarı verileri uygun hedefe ve başka hiçbir yere göndermez. Geleneksel sniffers'ı kandırmak için yaygın olarak kullanılan bir başka teknik ise transit halindeki verileri şifrelemektir. Saldırganlar şifreleme anahtarlarına sahip değilse, ağdan alınan verilerin içeriğini belirleyemezler. En popüler şifreleme protokollerinden ikisi, Web trafiğini güvenliğini sağlamak için en sık kullanılan Güvenli Yuva Katmanı (SSL) ve sistemlere komut satırı kabuğu erişimini korumak için en sık kullanılan Güvenli Kabuk'tur (SSH).

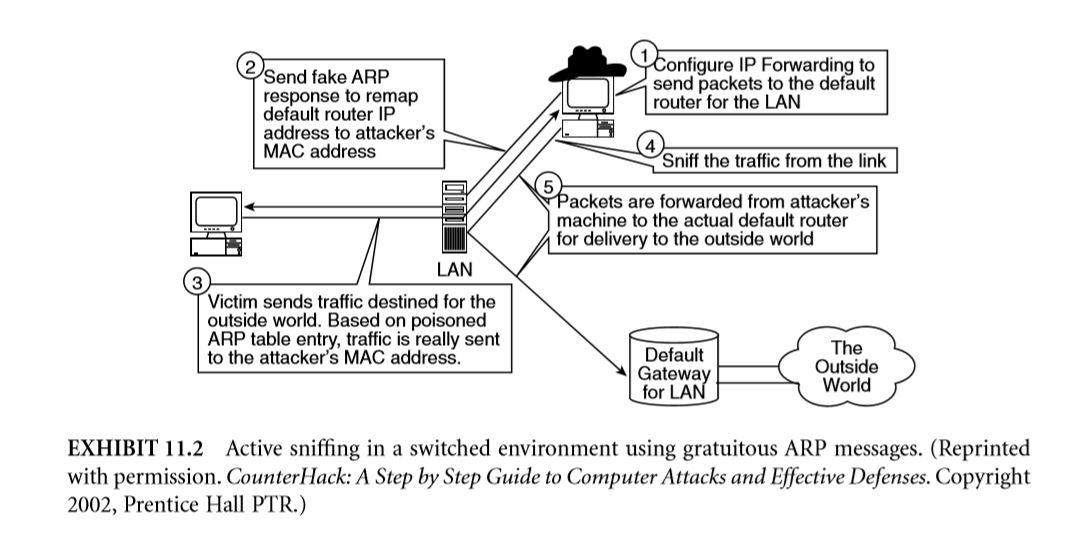
# 5.2. Aktif Snifing ile Antenin Yükseltilmesi

Pasif keskin nişancılara karşı savunmaları dağıtmada etkili ve faydalı olsalar da, saldırganlar onları engellemek için çeşitli teknikler geliştirmiştir. Topluca aktif engelleme olarak bilinen bu teknikler, bir saldırganın başka türlü çözülmemesi gereken verileri almasına izin vermek için ağa trafik enjekte etmeyi içerir. Mevcut olan en yetenekli aktif tarama programlarından biri, http://www.monkey.org/~dugsong/dsniff/ adresinde bulunan Dsniff'tir. Biri, Dsniff’in, bir ağa trafik enjekte ederek, MAC adresleri sızması, sahte ARP trafiği, sahte DNS yanıtları ve SSL’ye karşı ortadaki saldırılar dahil olmak üzere çeşitli ağlara enjekte edilmesi için çeşitli yöntemleri araştırır.

# 5.3. MAC Adreslerinin Taşması

Bir Ethernet anahtarı, medya erişim kontrolü (MAC) adresine dayanarak bir LAN üzerinde trafiği nereye göndereceğinizi belirler. MAC adresi, dünyadaki her Ethernet kartına atanan benzersiz bir 48 bitlik sayıdır. MAC adresi, LAN'a bağlı her sistem için benzersiz ağ arayüzü donanımını gösterir. Bir Ethernet anahtarı, anahtardaki hangi fişlerin hangi MAC adresleriyle ilişkili olduğunu öğrenmek için LAN üzerindeki trafiği izler. Örneğin, anahtar, bir numaralı fiş üzerindeki MAC adres AA: BB: CC: DD: DD: EE: FF'den gelen trafiği görecektir. Anahtar bu bilgiyi hatırlayacak ve bu MAC adresi için yazılan verileri sadece anahtardaki ilk fişe gönderecektir. Benzer şekilde, anahtar LAN'daki diğer ağ arayüzleriyle ilişkili MAC adreslerini otomatik olarak algılayacak ve onlara uygun verileri gönderecektir.

En basit ve aktif tarama tekniklerinden biri, LAN'ı sahte MAC adreslerine sahip trafiğe maruz bırakmayı içerir. Saldırgan, rastgele MAC adresleri olan paketler üretmek ve bunları switch'e beslemek için LAN üzerindeki bir makineye kurulu bir programı kullanıyor. Anahtar, gelen tüm MAC adreslerini hatırlamaya çalışacaktır. Sonunda, anahtarın bellek kapasitesi sahte MAC adresleriyle tükenir. Hafızası arttığında, bazı anahtarlar LAN'a bağlı tüm makinelere trafiğin gönderildiği bir moda geçer. Bu nedenle MAC modunu kullanarak bir saldırgan bir anahtarı bombalayabilir, böylece anahtar tüm LAN'lardaki tüm makinelere gönderir. Saldırgan daha sonra yerel ağdaki verileri almak için geleneksel bir dinleyiciyi kullanabilir.



# 5.4. Sahte ARP Trafiği

Bazı anahtarlar MAC altındaki bir modda, tüm trafiği LAN üzerindeki tüm sistemlere gönderdikleri bir modda başarısız olurken, diğer anahtarlar açılmaz. Bir kaynak sırasında, bu anahtarlar, LAN üzerinde otomatik olarak belirlenen ilk MAC adresleri kümesini hatırlar ve bu adresleri alan süresi boyunca kullanır. Saldırgan, anahtarı bastırmak için bir MAC düğmesini başlatamaz. Bununla birlikte, saldırgan, Adres Çözümleme Protokolü'ne (ARP) dayanarak başka tür bir trafik enjekte ederek hala böyle bir LAN'a zarar verebilir.

ARP, Internet Protokolü (IP) adreslerini LAN üzerindeki MAC adresleriyle eşlemek için kullanılır. Bir makine LAN üzerindeki başka bir sisteme gönderilecek verilere sahip olduğunda, hedefin IP adresi için bir paket oluşturur; Bununla birlikte, IP adresi sadece hedef makinedeki bir yapılandırma ayarıdır. Paketin gönderileceği gönderen makinenin, LAN üzerinde hangi donanım aygıtına gönderileceğini nasıl belirleyeceği? ARP cevaptır. LAN üzerindeki bir makinenin IP adresi 10.1.2.3 için belirlenmiş bir pakete sahip olduğunu varsayalım. Paketli makine, hangi ağ arayüzünün IP adresi 10.1.2.3 ile ilişkili olduğunu soran LAN üzerinde bir ARP isteği gönderir. Bu IP adresine sahip makine, özünde, “IP Adresi 10.1.2.3, MAC adresi AA: BB: CC: DD: DD: EE: FF.” İle ilişkilendirilir. Diyerek bir ARP yanıtı iletecektir. IP adresinin MAC adresine eşleştirilmesini, ileride başvurmak üzere ARP tablosu adı verilen yerel bir tabloda saklar. Paket daha sonra bu MAC adresi ile ağ arayüzüne teslim edilecektir. Bu şekilde, ARP IP adreslerini MAC adreslerine dönüştürmek için kullanılır, böylece paketler LAN üzerindeki uygun ağ arayüzüne iletilebilir. LAN üzerinde ek ARP trafiği ihtiyacını en aza indirmek için sonuçlar sistemin ARP tablosunda saklanır.

ARP, "bedava ARP" olarak adlandırılan bir yetenek için destek içerir. Ücretsiz ARP ile, hiçbir makine bir ARP isteği göndermemiş olsa da, bir makine bir ARP yanıtı gönderebilir. LAN'daki performansı iyileştirmeye yardımcı olmak için çoğu sistem ARP tablolarındaki ARP girişleri için susamıştır. Başka bir aktif snifing formunda, bir saldırgan, Ek 11.2'de gösterildiği gibi değiştirilmiş bir LAN'ı sniflemek için trafiği yönlendirmek için sahte ARP mesajlarını kullanır. Sergi için, saldırganın LAN'daki makinesi siyah bir şapka ile belirtilir. Ek 11.2'de gösterilen bu saldırının adımları:

1. Saldırgan, saldırganın LAN üzerindeki makinede IP iletimini etkinleştirir. Anahtarla siyah şapka makinesine yönlendirilen tüm paketler, LAN için varsayılan yönlendiriciye yönlendirilecektir.

2. Saldırgan, hedef makineye bedava bir ARP mesajı gönderir. Saldırgan, bu makineden dış dünyaya gönderilen trafiği koklamak istiyor. Ücretsiz ARP mesajı, LAN için varsayılan yönlendiricinin IP adresini, saldırganın kendi makinesinin MAC adresine eşleyecektir. Hedef makine bu sahte ARP mesajını kabul eder ve ARP tablosuna girer. Hedefin ARP tablosu şimdi yanlış girdiyle zehirlendi.

3. Hedef makine, dış dünya için hedeflenmiş trafik gönderir. LAN için varsayılan yönlendiriciyle ilişkili MAC adresini belirlemek için ARP tablosuna başvurur. ARP tablosunda bulunan MAC adresi saldırganın adresidir. Dış dünya için tüm veriler saldırganın makinesine gönderilir.

4. Saldırgan, trafiği hattan kokluyor.

5. Adım 1'de etkinleştirilen IP iletme özelliği, tüm trafiği saldırganın makinesinden LAN için varsayılan yönlendiriciye yönlendirir. Varsayılan yönlendirici trafiği dış dünyaya iletir. Bu şekilde, kurban dış dünyaya trafik gönderebilecek, ancak dışarı çekilmek için saldırganın makinesinden geçecek.

Bu adım dizisi, saldırganın dış dünyaya giden tüm trafiği hedef sistemden görmesini sağlar. Bu teknik için saldırganın anahtarı değiştirmediğini unutmayın. Saldırgan, mağdurun ARP tablosunu değiştirerek değiştirilmiş LAN'ı koklayabiliyor. ARP trafiği ve ilgili MAC adres bilgileri yalnızca bir LAN üzerinden iletildiğinden, bu teknik yalnızca saldırgan hedef sistemle aynı LAN üzerindeki bir makineyi kontrol ettiğinde çalışır.

# 5.5. Sahte DNS İstemcisi

Bir LAN'ın ötesine trafik koklamak için bir ağa paket enjekte etme tekniği, Alan Adı Sistemini (DNS) değiştirmeyi içerir. ARP bir LAN üzerinde IP adreslerini bir LAN üzerindeki MAC adresleriyle eşlemek için kullanılırken, DNS bir ağ üzerinde alan adlarını IP adreslerine eşlemek için kullanılır. Bir kullanıcı bir web tarayıcısına www.skoudisstuff.com adresini girme gibi bazı istemci yazılımlarına bir alan adı girdiğinde, kullanıcının sistemi bir DNS sunucusuna bir sorgu gönderir. DNS sunucusu genellikle ağ üzerinde farklı bir LAN'da bulunur. Sorgu alındıktan sonra, DNS sunucusu yapılandırılmasında uygun bilgiyi arar ve kullanıcının makinesine 10.22.12.41 gibi bir IP adresi içeren bir DNS yanıtı gönderir. DNS sunucusu, alan adını kullanıcının IP adresine eşleştirir. Saldırganlar müşteriye sahte DNS yanıtları göndererek trafiği yönlendirebilirler. Kibar bir DNS yanıtı gibi bir şey olmamasına rağmen, hedef sistemle DNS sunucusu arasında herhangi bir ağa oturan bir saldırgan, DNS sorgularını satırdan çekebilir. Bir istemciden bir DNS sorgusu göründüğünde, saldırgan, istemciye, saldırganın makinesinin IP adresini içeren sahte bir DNS yanıtı gönderebilir. Kullanıcıların makinesindeki istemci yazılımı, istenen sunucuyla iletişim kurduğunu düşünerek paketleri bu IP adresine gönderir. Bunun yerine, bilgiler saldırganın makinesine gönderilir. Saldırgan, geleneksel bir sniffer kullanarak bilgileri görüntüleyebilir ve trafiği hedeflenen yere aktarabilir.

# 5.6. SSL Saldırısı

Bir ağa sahte DNS yanıtları enjekte etmek, genellikle güvenli Web erişimi için kullanılan SSL gibi şifreleme protokollerine karşı ortada bir saldırı oluşturmak için kullanıldığında özellikle güçlü bir tekniktir. Esasen, saldırgan, saldırganın makinesinde yeni bir SSL oturumu oluşturmak için hedefe sahte bir DNS yanıtı gönderir. Sergi 11.3'te vurgulandığı gibi, saldırgan iki şifreleme oturumu ayarlamak için özel bir aktarma aracı kullanır: biri istemci ile saldırgan arasında, diğeri saldırgan ile sunucu arasında. Veriler bu oturumlar arasında hareket ederken, saldırgan açık metni görüntüleyebilir. Sergi 11.3'te gösterilen adımlar şunları içerir:

1. Saldırgan, sahte DNS yanıtları gönderen bir araç olan Dsniff’in dnsspoof programını etkinleştirir. Ek olarak, saldırgan, Web Monkey-in-the-Middle'ın kısaltması olan "webmitm" adlı başka bir Dsniff aracını etkinleştirir. Bu araç özel bir SSL geçişi uygular.

2. Saldırgan, kurban makinesinden bir DNS sorgusu gözlemler ve sahte bir DNS yanıtı gönderir. Sahte DNS yanıtı, saldırganın makinesinin IP adresini içerir.

3. Mağdur DNS cevabını alır ve cevabın içerdiği IP adresiyle bir SSL oturumu açar.

4. Saldırganın makinesinde çalışan webmitm aracı, kurban makine ile bir SSL oturumu ve istemcinin erişmek istediği gerçek Web sunucusuyla bir başka SSL oturumu kurdu.

5. Mağdur, SSL bağlantısı üzerinden veri gönderir. Webmitm aracı, kurbanla olan SSL bağlantısından gelen trafiği şifresini çözer, saldırgan için gösterir ve trafiği harici Web sunucusuna geçiş için şifreler. Harici Web sunucusu trafiği alır, ortadaki bir kişinin saldırısının gerçekleştiğinin farkına varmaz.

# 5.7. Aktif Snifing Tekniklerine Karşı Savunma

Bir saldırganın, ağlama araçlarını kullanarak bir ağdan her türlü faydalı bilgiyi nasıl alabileceğini gördükten sonra, bu saldırılara karşı nasıl bir savunma yapabilir? İlk olarak, mümkün olduğunda, ağ üzerinden iletilen verileri şifreleyin. Web trafiği için SSL, şifreli oturum açma oturumları ve dosya aktarımı için SSH, şifreli e-postalar için S / MIME ve ağ katmanı şifrelemesi için IPSec gibi güvenli protokolleri kullanın. Kullanıcıların, hem bilgileri hem de farkındalık bakış açısıyla hassas bilgileri korumak için bu araçları kullanması için donanımlı olması gerekir. Sistem yöneticilerinin, ağ yöneticilerinin ve güvenlik personelinin iş faaliyetlerini yürütmek için güvenli protokolleri anlamaları ve kullanmaları özellikle önemlidir. Asla güvenlik duvarına, yönlendiricilere, hassas sunuculara veya ortak anahtar altyapı (PKI) sistemlerine telnet yapmayın! Bir saldırganın telnet'in açık metin olarak ilettiği bir şifreyi engellemesi çok kolaydır. Ayrıca, tarayıcıdan ve SSH istemcisinden gelen uyarı mesajlarına dikkat edin. Güvenilmeyen bir sertifika ile oluşturulan bir SSL oturumu kullanarak ağ üzerinden hassas bilgiler göndermeyin. SSH istemcisi, sunucunun genel anahtarının gizemli bir şekilde değiştiği konusunda uyarırsa, araştırmaya ihtiyaç vardır.

Ek olarak, gerçekten de hub'lardan kurtulmayı düşünmelisiniz, çünkü kolayca koklanamayacak kadar kolaydırlar. Maliyet hub'lardan daha yüksek olsa da, anahtarlar yalnızca güvenliği artırmakla kalmaz aynı zamanda performansı da artırır. Anahtarlamalı bir ağa tam bir geçiş yapmak mümkün değilse, en azından kritik ağ segmentlerinde, özellikle de DMZ'de anahtarlamalı Ethernet kullanmayı düşünün. Son olarak, çok hassas sistemler ve veriler içeren ağlar için, MAC problemlerini ve sahte ARP mesajlarını önlemek için her bir port portunu makinenin belirli MAC adresi ile o portu kullanarak ayarlayarak portlarınızdaki güvenliği sağlayın. Ayrıca, İnternet DMZ'ler gibi son derece hassas ağlar için, uç makinelerdeki statik ARP tablolarını kullanın ve LAN adresindeki tüm sistemler için MAC adreslerini sabit kodlayın. Bir anahtar ve sabit kodlanmış ARP tablolarındaki bağlantı noktası güvenliği, yönetimi zor olabilir çünkü bileşenleri değiştirmek veya hatta Ethernet kartları, birçok sistemde depolanan MAC adreslerinin güncellenmesini gerektirir. İnternet DMZ'leri gibi çok hassas ağlar için bu güvenlik seviyesi gereklidir ve uygulanmalıdır.

Section 1.5.3. Social Engineering: The Forgotten Risk - Sosyal Mühendislik: Unutulmuş Risk

Mustafa ALACA

130757037

# 6. Social Engineering: The Forgotten Risk - Sosyal Mühendislik: Unutulmuş Risk

Bilgi ve bilgi teknolojisi güvenliği hakkında düşündüğümüzde, ortak dikkatimizi bu güvenlik zincirinin belirli teknik alanlarına odaklamalıyız.Çünkü sistemler en zayıf halkaları kadar güçlüdürler.

Bu bölüm, bu saldırının nasıl çalıştığını, kullanılan yaygın yöntemlerin neler olduğunu ve uygun eğitim, farkındalık eğitimi ve diğer kontrollerle sosyal mühendislik riskini nasıl azaltabileceğimizi inceleyerek sosyal mühendisliğe ışık tutmaya çalışmaktadır.

Bunun “nasıl yapılır” bölümü olması amaçlanmamıştır, bunun yerine , bu tür saldırıların ayrıntılarının ve sosyal mühendislik mağduru olmanın nasıl önlenebileceğinin tartışılmasıdır.Bu bölüm, bu saldırının nasıl çalıştığını, kullanılan yaygın yöntemlerin neler olduğunu ve uygun eğitim, farkındalık eğitimi ve diğer kontrollerle sosyal mühendislik riskini nasıl azaltabileceğimizi inceleyerek sosyal mühendisliğe ışık tutmaya çalışmaktadır. Bunun “nasıl yapılır” bölümü olması amaçlanmamıştır, bunun yerine , bu tür saldırıların ayrıntılarının ve sosyal mühendislik mağduru olmanın nasıl önlenebileceğinin tartışılmasıdır.Bu bilgilerin hiçbiri gizli değildir; toplumun belli kesimleri tarafından zaten bilinir. Bu nedenle, bilgi güvenliği uzmanlarının riski azaltmak için sosyal mühendislikten ve güvenlik kontrollerinden haberdar olmaları da önemlidir .

# 7. Sosyal Mühendisliğin Tanımlanması

Sosyal mühendisliğin ne olduğunu anlamak için önce neyin tartışıldığını net bir şekilde tanımlamak önemlidir. “Sosyal mühendislik” terimi yeni bir terim değildir. Sosyal kontrol alanından geliyor. Sosyal mühendislik, arzu edilen bir sonucu elde etmek için bir toplumu yeniden tanımlama sürecine (veya daha doğrusu bir mühendislik topluluğuna) atıfta bulunabilir.Bu terim aynı zamanda insanların davranışlarını öngörülebilir bir şekilde, genellikle yeni bir sisteme uymaları için değiştirmeye teşebbüs etme sürecini de ifade edebilir .

Bu noktada sosyal mühendislik probleminin görünür büyüklüğü hakkında bazı bilgiler eklemek çok ilginç olurdu. Ne yazık ki, bu amaç için kullanılacak çok az veri var. Bilgi güvenliği alanındaki sık sık sosyal mühendisliğe yapılan atıflara rağmen, bu tür bir saldırı hakkında doğrudan bir tartışma yapılmamıştır.

# 8. Sosyal Mühendislik Neden İş Yapıyor?

Sosyal mühendislik saldırılarının başarısı temel olarak iki faktörden kaynaklanıyor:

* Temel insan doğası
* İş ortamı

# 8.1.İnsan Doğası

Bir sosyal mühendislik saldırısına kurban olmak, istihbaratla ve insan olmakla ilgili, biraz saf olmayan ve bu tür bir saldırı ile başa çıkmak için uygun bir zihinsel düzen ve eğitime sahip olmakla ilgisi yoktur.

İnsanlar, çoğunlukla, doğası gereği güveniyor ve işbirliği yapıyorlar.

Sosyal psikoloji çalışmalar, doğru duruma konan ve yetenekli bir kişiyle ilgilenen hemen hemen herkesin belirli bir şekilde davranması veya genellikle diğer durumlarda yapamayacağı bilgileri ifşa etmesinin etkilenebileceği sonucuna varmıştır.Bu çalışmalar aynı zamanda otorite içinde olan veya otorite içinde olma havasına sahip kişilerin diğer insanları kolayca korkuttuklarını da tespit etti.

# 8.2.İş Ortamı

İnsan doğası, birleşme ve satın almaların şu andaki iş eğilimi, teknolojideki hızlı gelişmeler ve geniş alan ağlarının yaygınlaşması iş ortamını sosyal mühendisliğe elverişli hale getirmiştir. Günümüzün iş dünyasında, bir kişinin kendi kuruluşundan, tedarikçilerinden, tedarikçilerinden ve müşterilerinden oluşan kişiler de dahil olmak üzere, düzenli olarak uğraştığı insanlarla hiçbir zaman tanışmaması normal değildir.

Çalışanlar için telekomünikasyon teknolojilerinin yaygın olarak benimsenmesiyle yüz yüze insan etkileşimi daha da nadir hale geliyor. Günümüz pazarında, bir kuruluş için çalışabilir ve birkaç istisna dışında, nadiren ofise ayak basabilir. Çalışma ortamımızdaki insanlarla olan bu soyutlama katmanına rağmen, aslında hiç karşılaşmadığımız kişiler dahil olmak üzere insanlara olan temel güvenimiz oldukça sağlam kaldı.Çalışanlar işe alınırken, görevleri yerine getirirken güvenlik konusunda ne kadar bilgisi olmasına bakılmaz ve bu da büyük bir hatadır.Bu sosyal Mühendislik tehdidi etkili bir şekilde ele almak için değişmesi gereken paradigmadır..Sosyal Mühendislik Saldırıları

Sosyal mühendislik saldırıları aşamalı bir yaklaşımı takip etme eğilimindedir ve çoğu durumda saldırılar istihbarat teşkilatlarının hedeflerine nasıl sızdığını gösterir.

Bu aşamalar ise :

İstihbarat toplama

Hedef seçme

Saldırı

# 8.3. İstihparat Toplama

Başarılı bir sosyal mühendislik saldırısının anahtarlarından biri bilgidir. Bir şirket çalışanı, bir satıcı temsilcisi veya bazı durumlarda bir düzenleyici veya yasa uygulama organının bir üyesi gibi konuşabilmek için bir kuruluş ve personeli hakkında yeterli bilgi toplamak şaşırtıcı derecede kolaydır.Saldırgan bu bilgileri şirketlerin web sitelerinde şirket bilgilerini (şube bilgisi, telefon dizini ,kuruluş amaçları vb.) , ve çöplüklerini araştırarak ulaştığı fatura, yazışmalar, el kitapları vb. saldırgana çoğu gerekli bilgiyi sağlar.Saldırganın bu aşamadaki amacı, meşru bir çalışan, yüklenici, satıcı, stratejik ortak veya bazı durumlarda bir kolluk görevlisi gibi konuşabilmek için olabildiğince fazla bilgi edinmektir.

# 8.4. Hedef Seçme

Uygun miktarda bilgi toplandıktan sonra, saldırgan kurum personelinde gözle görülür zayıflıklar arar.En yaygın hedef yardım masası personelidir, çünkü bu profesyoneller yardım vermek için eğitilmişlerdir ve genellikle parolaları değiştirebilir, hesap oluşturabilir, hesapları yeniden etkinleştirebilir.Çoğu saldırganın amacı ya hassas bilgileri toplamak ya da bir sisteme ayak basmaktır.

Saldırganlar, bir misafir düzeyinde bile erişime sahip olduklarında, ayrıcalıklarını arttırmanın, daha yıkıcı saldırılar başlatmanın ve izlerini gizlemenin nispeten kolay olduğunu fark eder. İdari asistanlar sıradaki en yaygın kurbanlardır. Bu, büyük ölçüde, bu bireylerin normalde üst düzey yönetim üyeleri arasında akan çok miktarda hassas bilgiye sahiptirler.İdari asistanlar, bir saldırı noktası olarak ya da organizasyondaki etkili kişilerin isimleriyle ilgili ek bilgi .toplamak için kullanılabilir.

# 8.5. Saldırı

Gerçek atak genellikle biz en yaygın bir diyeceğimiz dayanmaktadır Bu üç kategoriye ayrılır :

* Mağdurun egosuna saldırılar
* Saldırıları duygular yararlanmak olduğunu sempati veya empati
* Yıldırıma dayanan saldırılar.

# 8.5.1. Ego Attacks

İlk saldırı türünde - ego veya kibir saldırıları - saldırgan en temel insan özelliklerinden bazılarına hitap eder.Herkesin genellikle ne kadar zeki olduğunu duyması onu mutlu eder.Saldırganlarda bunu yapıyor seçtiği kurbanının egosunu tatmin ederek şirket bilgilerini öğrenmeye çalışır ve genellikle öğrenirlerde.Kurban bu kişinin saldırgan olduğunun farkına varmayacaktır bile çünkü egosu tatmin edilir ve o anlık saldırganı çok iyi biri olarak tanır.

# 8.5.2. Sempati Atakları

Sadırgan genellikle ,yeni işe alınan bir çalışan gibi davranır.İstihbarat aşamasının önemi burada belirginleşir, çünkü saldırganlar, kurbanla , oldukları gibi olduklarına dair bir güven düzeyi oluşturmak zorunda kalacaklardır.Bu, isim bırakarak, uygun jargonu kullanarak veya organizasyon bilgisini göstererek yapar.Saldırgan genellikle işinin acele olduğunu söyleyerek bunu yapmaya çalışır .Mesela bilgi işlemi arayarak yeni işe girdiğini söyler , bilgi toplaması sayesinde elde ettiği kullanıcı adının şifresini ister , bu şifreyi aldığında ise sisteme giriş yapar ve erişim denetimi yetersiz ise sistemde açık aramaya başlar.

# 8.5.3. Sindirme Saldırıları

Üçüncü kategoride, saldırganlar otorite figürleri ,organizasyonda etkili bir kişi , kolluk kuvvetleri gibi davranırlar. Saldırganlar, kurban olarak organizasyonda kendini tanıttığı seviyenin altındaki birkaç seviyeyi hedefleyecektir.Saldırgan, parola sıfırlama, hesap değişikliği, sistemlere erişim veya hassas bilgiler için bir tür istekte bulunmak için makul bir neden oluşturur.Saldırganlar, zamanın önemli olduğu ve standart prosedür ne olursa olsun onu atlatmaları gereken senaryoları kullanırlar. Direnişle karşı karşıya kalırsa, saldırganlar mağdurlarını kendilerine yönelik yaptırımları tehdit ederek işbirliğine zorluyorlar.

# 9. Riski Azaltma

Sosyal mühendislik saldırısının türü ne olursa olsun, başarı oranı endişe verici derecede yüksek. Sosyal mühendislik saldırılarının riski ve etkisi yüksektir. Bu saldırıların izini sürmek ve bazı durumlarda tespit etmek zordur.Saldırganın meşru bir hesap üzerinden erişim kazanması durumunda, çoğu durumda kontroller ve alarmlar, sistem söz konusu olduğunda yanlış bir şey yapmadıkları için asla etkinleştirilmez.Sosyal mühendislik yapmak bu kadar kolaysa, kuruluşlar kendilerini bu saldırıların risklerine karşı nasıl korurlar? Sosyal mühendislik riskini azaltmak için kuruluşların, personellerini bilgi güvenliği tehditleri ve potansiyel saldırıları nasıl tanıyacakları konusunda etkin bir şekilde eğitmeleri gerekir. Bu saldırıların kontrolü, tartışmayı izleyen eğitim, farkındalık, eğitim ve diğer kontrollerde bulunabilir.Sosyal mühendislik, bilgi güvenliği zincirindeki en zayıf halkaya odaklanıyor (insanlar).