**9 - Uzaktan Erişime Güvenli Giriş**

Christina M. Bird, Ph.D, CISSP

Geçtiğimiz on yılda, şirket ağlarına uzaktan erişim sağlama ve kontrol etme sorunu, ağ yöneticileri ve bilgi güvenliği uzmanlarının karşılaştığı en zorlu sorunlardan biri haline geldi. Bilgi temelli işletmeler küresel ekonominin daha büyük ve daha büyük bir bölümü haline geldikçe, “iş” in doğası değişiyor. “İşler”, fabrika, ofis veya mağaza gibi iyi tanımlanmış bir yerde, çalışanların göreceli olarak organize edilen hiyerarşileri arasında önceden belirlenmiş zamanlarda gerçekleşirdi. Ama şimdi, “iş” her yerde gerçekleşiyor: tüm dünyada, günün her saati, çalışanlar, danışmanlar, satıcılar ve müşteri temsilcileri arasında. Bir çalışan, oturma odasında kişisel bir bilgisayarla ve bir modemle çalışma hattında, montaj hattı olmadan, bir kabin veya görüşte bir yönetici olmadan verimli olabilir.

İnternet’in iş dünyasında ve kişisel yaşamda bir iletişim aracı olarak yaygın kabul görmesi, yeni bir bilgisayar kullanıcısı grubuna uzaktan erişim kavramını getirmiştir. İnternet erişiminin hız ve basitliğinin çalışma ortamlarına da çevrilmesini beklerler. Seyahat eden çalışanlar, kendi özel ağ bağlantılarının otel odasındaki, sanki evdeymiş gibi kusursuz bir şekilde çalışmasını ister. Bu, çoğunlukla ağ kurmanın temel iş için en iyi olduğu kuruluşlar dahilinde güvenilir ve verimli kurumsal uzaktan erişim sistemlerine olan talebi arttırır.

Bilgisayar kullanıcılarının özel bir ağda patlaması - şimdi sadece ofis çalışanlarını değil aynı zamanda telekomünikasyon şirketleri, danışmanlar, iş ortakları ve müşterileri de içeren - güvenli uzaktan erişimin tasarımını ve uygulamasını daha da zorlaştırıyor. En basit yerel alan ağlarında (LAN), tüm kullanıcılar ağdaki tüm kaynaklara sınırsız erişime sahiptir. Bazen, giriş ayrıcalıklarını kısıtlayarak, ana bilgisayar düzeyinde ayrıntılı erişim kontrolü sağlanır. Ancak, gerçek dünyadaki çoğu ortamda, muhasebe, insan kaynakları veya araştırma ve geliştirme gibi farklı verilere erişim sınırlı insan grupları ile sınırlandırılmalıdır. Bu kısıtlamalar ağdaki kaynakları fiziksel olarak izole ederek veya mantıksal mekanizmalar (yönlendirici erişim kontrol listeleri ve daha katı duvar teknolojileri dahil) aracılığıyla sağlanabilir. Özellikle fiziksel izolasyon, ağ kaynaklarına önemli ölçüde koruma sağlar ve bazen kasıtlı bir ağ güvenliği stratejisi olmadan da gelişir.

Uzak çalışanlara, danışmanlara, şubelere ve iş ortağı ağlarına bağlantılar, şirket içinde ve arasında iletişimi son derece verimli kılar; ancak şirket ağlarını ve hassas verileri geniş, potansiyel olarak güvenilmeyen bir kullanıcı topluluğuna ve yeni bir güvenlik açığına maruz bırakırlar. Çalışan olmayan kişilerin gizli bilgileri kullanmalarına izin vermek, veri sınıflandırma ve erişim kontrolü için katı şartlar yaratır. Çalışan olmayanlar için bir kurumsal güvenlik politikası uygulamak için bir ağ altyapısını yönetmek, çoğu ağ yöneticisi ve güvenlik yöneticisi için yeni bir zorluktur. Kuruluşun uzaktan erişim için makul iş gereksinimlerini kolaylaştırmak için güvenlik politikası uyarlanmalıdır. Aynı zamanda, politikalar ve prosedürler, gelişmiş bağlantının, şirket ağındaki veri gizliliği, bütünlüğü ve kullanılabilirliğinden ödün vermesine neden olma ihtimalini en aza indirmeye yardımcı olur.

Benzer şekilde, şirket şubesi ve müşteri destek grupları da uygun maliyetli, sağlam ve güvenli ağ bağlantıları talep etmektedir.

Bu bölümde kurumsal uzaktan erişim mimarisi için genel tasarım hedefleri, ortak uzaktan erişim uygulamaları ve sanal özel ağların (VPN'ler) kullanılmasıyla güvenli uzaktan erişim sağlamak için İnternet kullanımı ele alınmaktadır.

**Uzaktan Erişim için Güvenlik Hedefleri**

Tüm uzaktan erişim sistemleri, meşru kullanıcılar ve ana şirket kampüsünden uzakta bulunan siteler için uygun güvenlik politikalarına tabi özel olarak tutulan bilgisayar kaynaklarına bağlantı kurmak için tasarlanmıştır. Her biri kendine özgü güçlü ve zayıf yönleri olan bu tür sistemler var. Bununla birlikte, gizliliğin, veri bütünlüğünün ve kullanılabilirliğin korunmasının çok önemli olduğu bir ağ ortamında, güvenli bir uzaktan erişim sistemi aşağıdaki özelliklere sahiptir:

• Kullanıcıların ve sistemlerin güvenilir bir şekilde doğrulanması

• Belirli bilgisayar sistemlerine, dosyalara ve diğer ağ kaynaklarına erişimin kolay yönetilmesi için ayrıntılı bir denetim

• Gizli verilerin korunması

• Sistem kullanımının günlüğe kaydedilmesi ve denetlenmesi

• İşyeri ortamının daha verimli bir şekilde yeniden üretilmesi

• Maksimum sayıda uzak kullanıcı ve yere bağlantı

• Ekipman, ağ bağlantısı ve destek için minimum maliyet

**Uzak Kullanıcıların / Ana Bilgisayarların Güvenilir Kimlik Doğrulaması**

Bariz görünüyor, ancak, bilgisayardaki ve uzaktaki kullanıcılar arasındaki temel farkın, uzaktaki kullanıcıların orada olmadığı üzerinde durmaya değer. Küçük bir kuruluşta bile, minimum güvenlik gereksinimi olan birçok resmi olmayan kimlik doğrulama işlemi gün boyunca gerçekleşir. İş arkadaşları birbirlerini tanır ve tüm ofis boyunca belirli sistemleri kimlerin kullanması gerektiği konusunda bir anlayışa sahiptir. Benzer şekilde, şirketin sunucu odasına kimlerin girip çıkacağına dikkat ederlerse basit bir erişim kontrol mekanizması sağlayabilirler.

Yüksek güvenlik gereksinimi olan kurumlarda, bir çalışanın veya bir bilgisayarın fiziksel varlığı, kampüs içerisinde kullanılacak tanımlama, doğrulama ve erişim kontrolü mekanizmaları için birçok teknolojik olanak sağlar. Bunlar arasında güvenlik görevlileri, fotoğraf çalışanı kimlik kartları, güvenli alanlara anahtarsız giriş, diğer birçok araç var.

Güvenli bir uzaktan erişim sistemi, insan kullanıcıları için çeşitli güçlü kimlik doğrulama mekanizmalarını ve şirketler ve iş ortaklarının şubesi için makinelerin ve ağ geçitlerinin kimliklerini doğrulamak için dijital sertifikaları destekler.

**Granül Erişim Kontrolü**

İyi bir uzaktan erişim sistemi, ağ sistemleri ve saha dışı bir kullanıcı tarafından erişilebilecek kaynaklar üzerinde esnek bir kontrol sağlar. Yöneticiler, diğer her şeye erişimi reddederken uygun tüm iş amaçlarına erişim sağlamak için tahıl kontrolüne sahip olmalıdır. Bu, farklı kullanıcı türleriyle (çalışanlar, üçüncü taraf müteahhitleri vb.) Güven ilişkilerine dayanan çeşitli erişim politikalarının yönetilmesini sağlar. Erişim kontrol sistemi, kuruluşun güvenlik gereksinimlerini destekleyecek kadar esnek olmalı ve politikalar veya personel değiştiğinde kolayca değiştirilmelidir. Uzaktan erişim sistemi incelikle ölçeklenmeli ve şirketin erişim gereksinimleri geliştikçe daha karmaşık politikalar uygulamasına olanak sağlamalıdır.

Erişim kontrol sistemleri, ağ tabanlı erişim kontrol listeleri, statik yollar ve ana bilgisayar sistemi ve uygulama tabanlı erişim filtreleri dahil olmak üzere çeşitli mekanizmalardan oluşabilir. İdari arayüzler

çoklu erişim politikalarını yönetmenize yardımcı olmak için şablonları ve kullanıcı gruplarını, makineleri ve ağları destekleyebilir. Bu kontroller, farklı derecelerde, duvarlar, yönlendiriciler, uzaktan erişim sunucuları ve kimlik doğrulama sunucuları tarafından sağlanabilir. Güvenlik politikası talep ederse, bir ağın çevresinde ve dahili olarak dağıtılabilirler.

Uzaktan erişim sisteminin başlatılması, şirket ağında halihazırda mevcut olan güvenlik altyapısına zarar vermemelidir. Bir kuruluş zaten kullanıcı veya dizin tabanlı güvenlik denetimleri uygulamışsa (örneğin, Novell'in Netware Directory Hizmeti veya Windows NT etki alanlarına dayalı olarak), bu denetimlerle bütünleşen bir uzaktan erişim sistemi şirketin yatırımını ve deneyimini artıracaktır.

**Gizli Verilerin Korunması**

Genel veya yarı özel ağ altyapısını kullanan uzaktan erişim sistemleri (İnternet ve genel telefon ağı dahil), özel verilerin beklenmedik ellere düşmesi için birçok fırsat sağlar. İnternet, en yaygın olarak bilinen kamu ağıdır, ancak tek değildir. Özel Frame Relay bağlantıları ve uzaktan çevirmeli abonelik hizmetleri (birçok telekomünikasyon sağlayıcısı tarafından sunulan) bile aynı fiziksel devrelerdeki çeşitli konumlardan ve organizasyonlardan veri aktarır. Frame Relay sniffers, ağ yöneticilerinin özel sanal devreler üzerindeki trafiği incelemelerini sağlayan ve ağ geçidi güvenli bağlantılar arasında şaşırtıcı bir miktarda dinlenmeye izin veren emtia ağ cihazlarıdır. Bu sistemlerdeki paket sızıntı raporları, BUGTRAQ ve Firewall-Wizards gibi güvenlik posta listelerinde nispeten yaygındır.

İnternette yaygın olarak kabul edilen tehditler, diğer büyük ağlar ve ağ servisleri için de geçerlidir. Böylece, nominal olarak özel uzaktan erişim sistemlerinde bile - modem bankaları ve telefon hatları, kablo modem bağlantıları, Frame Relay devreleri - güvenlik konusunda bilinçli yöneticiler, güçlü şifreleme ve paket başına kimlik doğrulaması gerçekleştiren ekipmanları kullanacaklardır.

**Sistem Kullanımının Günlüğü ve Denetimi**

Güçlü kimlik doğrulama, şifreleme ve erişim kontrolü, kurumsal verilerin korunması için önemli mekanizmalardır. Ancak er ya da geç, her ağ, sistem arızalarından (donanım ya da yazılım), insan hatası ya da saldırısından kaynaklanan ya da kasıtlı bozulmalarla karşı karşıya kalır. Sistem kullanım günlüklerinin ayrıntılı bir şekilde tutulması sistem arızalarının giderilmesine yardımcı olur.

Eğer sorun giderme bir ağ problemine bilerek neden olduğunu gösteriyorsa, denetim bilgisi failin takibinde kritik öneme sahiptir. Kişinin kurumsal güvenlik politikası, yalnızca kullanıcıları uzaktan erişim sistemindeki bireysel eylemlerle ilişkilendirme yeteneği kadar iyidir - eğer biri kimin yaptığını söyleyemezse, o zaman kişi kuralları ihlal ettiğini söyleyemez.

Maalesef, uzaktan erişim ekipmanlarının çoğu, en iyi şekilde basit günlük kaydı yapar. , Kullanıcı adı saklamak başlangıç ​​zamanı ve çağrı süresi - - Çoğu durumda, seviye denetim çağrı kaydedilir, ancak uzak kullanıcı aslında ne yaptığını konusunda yeterli veri yoktur. Eğer şirket ortamı daha sıkı denetim izleri gerektiriyorsa, muhtemelen özel denetim sistemleri tasarlamak zorunda kalacaktır.

**İşyeri Ortamının Şeffaf Çoğaltılması**

Telekomünikasyon cihazları ve yol savaşçıları için uzaktan erişim, fiziksel olarak kendi konumlarında olsaydı, keyif alacakları aynı düzeyde bağlantı ve işlevsellik sağlamalıdır. Merkez şubesi, şirket merkezi ağlarına merkez kampüs ile aynı erişime sahip olmalıdır. Dahili ağ işteki çalışanlar tarafından serbestçe erişilebilirse, uzak çalışanlar aynı derecede erişimi bekler. Dahili ağ fiziksel veya mantıksal güvenlik kısıtlamalarına tabi ise, uzaktan erişim sistemi bu kısıtlamaların uygulanmasını sağlamalıdır. Uzak sistemlerde tam işlevsellik bulunmuyorsa, iş açısından kritik öneme sahip kaynak ve uygulamalara öncelik verilmelidir, aksi takdirde insanlar bunu kullanmaz.

Şeffaf bağlantı sağlamak, göründüğünden daha zor olabilir. Küçük bir organizasyonda bile, kişisel çalışma alışkanlıkları çalışanlardan çalışanlara büyük farklılıklar gösterir ve bu farklılıkların uzaktan erişim kullanımını nasıl etkileyebileceğini tahmin etmek problemlidir. Örneğin, bir UNIX dosya sunucusunda depolanan verilere erişimi düşünün. UNIX iş istasyonlarına sahip çalışanlar, bu dosyalara erişmek için Ağ Dosya Hizmeti (NFS) protokolünü kullanır. NFS, düzgün çalışması için kendi özel ağ bağlantıları, sunucu yapılandırmaları ve güvenlik ayarlarını gerektirir. Windows tabanlı iş istasyonlarına sahip çalışanlar, aynı dosyalara erişmek için muhtemelen Sunucu Mesaj Veriyolu (SMB) protokolünü kullanır. SMB kendi konfigürasyon dosyalarını ve güvenlik ayarlarını gerektirir. Kurumsal uzaktan erişim sistemi NFS'yi aktaramadığında.

**Uzak Kullanıcılara ve Konumlara Bağlantı**

Sağlam ve uygun maliyetli bir uzaktan erişim sistemi, telefon hatları, kalıcı özel ağ bağlantıları, isteğe bağlı arama ağ bağlantıları ve İnternet dahil olmak üzere çeşitli mekanizmalar üzerindeki bağlantıları destekler. Bu, uzaktan erişim mimarisinin, tüm bağlantı mekanizmalarının herhangi bir zamanda kullanılmakta olup olmadığına bakılmaksızın, ağ altyapısı geliştikçe kullanışlılığını korumasını sağlar.

Birden fazla bağlantı tarzı desteği, kurumsal ağa çeşitli konumlardan erişim için bir çerçeve oluşturur: oteller, evler, şirketler şubesi, iş ortakları ve müşteri siteleri, yerel veya uluslararası. Bu esneklik ayrıca sisteme artıklık ve performans ayarlama yetenekleri ekleme görevini de basitleştirir.

Halihazırda konuşlandırılmış uzaktan erişim sistemlerinin çoğu, en azından çalışan ve istemciden sunucuya uzaktan bağlantı için, ağ protokolü olarak TCP / IP kullanmaktadır. Daha küçük bir kesim IPX, NetBIOS / NetBEUI ve diğer LAN protokolleri için destek gerektirmeye devam ediyor; SNA, DECNet ve daha eski servisleri bile daha az destekliyoruz. TCP / IP çoğu modern bilgisayar işletim sisteminde destek avantajı sunar; Çoğu kurumsal uygulama TCP / IP'yi ağ protokolü olarak kullanır veya trafiğinin TCP / IP ağları üzerinden kapsüllenmesine izin verir. Bu bölüm, TCP / IP tabanlı uzaktan erişim ve özel güvenlik kaygıları üzerine odaklanmaktadır.

**Maliyetleri En Aza İndir**

İyi bir uzaktan erişim çözümü, donanım, ağ kullanımı ve destek personelinin maliyetlerini en aza indirecektir. Elbette, uzaktan erişim, uygun yatırım getirisi ve uygun personel bütçeleri için uygun harcamaların belirlenmesinin kuruluştan organizasyona farklılık gösterdiğini ve kaynak kaybına duyarlılık, ağ ve güvenlik tasarımında kurumsal uzmanlık ve Sanayiye bağlı olarak olası düzenleme sorunları.

Herhangi bir uzaktan erişim uygulamasında, toplam maliyete en yüksek tek katkı kalıcı devrelere yapılan ödemeler, telefon kapasitesi, özel ağ bağlantıları veya İnternet erişimi olabilir. İş gereklilikleri, tipik olarak uzak kullanıcıların beklenen yerlerine, gereken LAN-LAN bağlantılarının sayısına ve verimlilik ile eşzamanlı bağlantılara ilişkin beklentilere bağlı olarak, gerekli devre tipleri kombinasyonunu belirleyecektir. Ekipman, yazılım ve kurulum için bir defalık ücretler, özellikle yüksek güvenlikli bir ortamda, uzaktan erişim mimarileri arasındaki nadiren temel farklılıklardır. Bununla birlikte, uzaktan erişim seçenekleri arasında adil bir şekilde karar vermek ve gelecekteki büyümeyi planlamak için, maliyet tahminlerinde aşağıdaki bileşenleri göz önünde bulundurun:

• Bir kerelik donanım ve yazılım maliyetleri

• Kurulum ücretleri

• Bakım ve yükseltme maliyetleri

• Ağ ve telefon devreleri

• Kurulum ve günlük yönetim için gereken personel

Uzaktan erişim mimarilerinin tümü bir kuruluşun işletme gereksinimlerini minimum para ve çabayla karşılamayacak, bu nedenle ilk aşamalarda planlama yapmak çok önemlidir.

Bu yazının yazıldığı sırada, bireyler için İnternet erişimi, özellikle uzun mesafeli telefon ücretlerinin maliyeti ile karşılaştırıldığında nispeten ucuzdur. Evde İnternet erişim maliyeti, kullanım başına hesaplamalar yerine aylık ücrete dayalı olduğu sürece, özellikle seyahat eden çalışanlar için bireysel uzaktan erişim sağlamak için İnternet kullanımı ekonomik olarak cazip kalacaktır. Bir kurumun genel İnternet stratejisine bağlı olarak, şube ve merkez arasındaki özel ağ bağlantılarının güvenli İnternet bağlantılarıyla değiştirilmesi, birkaç yıl boyunca üçte bir ila üç buçuk arasında tasarruf sağlayabilir. Uzaktan erişim için bu devasa maliyet düşüşü, güvenli sanal özel ağların kurumsal bir uzaktan erişim altyapısı olarak değerlendirilmesinde birincil motivasyondur. Ancak, bir kuruluşun İnternet ağları ve güvenlik sistemlerinin konuşlandırılmasında deneyimli teknik kadroya sahip olmaması durumunda, devam eden devre maliyetleri açısından algılanan tasarrufların idari personeli işe alma ve eğitme girişiminde kolayca kaybedilebileceğini unutmayın.

Bu gereksinimler ışığında uzaktan erişim altyapılarını değerlendirmek güvenlik mimarının sorumluluğundadır. Uzaktan erişim ekipmanı ve servis sağlayıcıları ekipmanlarının performansı, beklenen idari ve bakım gereklilikleri ve fiyatlandırma hakkında bilgi sağlayacaktır. Telefon ve ağ bağlantısındaki fiyatlandırmayı düzenli olarak inceleyin; telekomünikasyon pazarı hızla değişiyor ve erişim maliyetleri coğrafya, ses / veri iletişimi hacmi ve şirket birleşmeleri olasılığı gibi çeşitli faktörlere karşı son derece hassas.

İyi bir uzaktan erişim sistemi ölçeklenebilir, uygun maliyetli ve desteklemesi kolaydır. Ölçeklenebilirlik sorunları arasında donanım ve yazılım geliştirmeleri yoluyla uzaktan erişim sunucularında (özel ağa açılan kapılar) kapasite artışı; özel ağa ağ bant genişliğinin (veri veya telefon hatları) arttırılması; ve altyapıyı ve uzak kullanıcıları destekleyecek personeli sağlamak. Eğer sistem görev açısından kritik bir bağlantı sağlamak için kullanılacaksa, dağıtımın ilk aşamalarından itibaren güvenilir, ölçülebilir verimlilik ve artıklık ile tasarlanması gerekir. Kritik bağlantıların ortaya çıkacağı her yerden uzaktan erişimin yedekleme yöntemleri gerekecektir.

Her uzaktan erişim sisteminin mutlaka bu özelliklerin her birine sahip olmadığını (veya gerektirdiğini) unutmayın. Herhangi bir şirket ortamında, güvenlik kararları önceden var olan politikalara, algılanan tehdide, potansiyel kayıplara ve yasal gerekliliklere dayanmaktadır - ve diğerleri gibi uzaktan erişim kararları, belirli bir kuruluş ve ağ gereksinimlerine özel olacaktır. Nispeten sabit bir çalışan popülasyonuna sahip 30 ila 40 seyahat satış ekibini destekleyen bir kuruluşun, esneklik ve ölçeklenebilirlik için minimum gereksinimleri vardır - özellikle de uzak kullanıcıların tümü güvenilir çalışanlar olduğu ve yalnızca bir güvenlik politikası uygulandığı için. Birden fazla lokasyona sahip büyük bir organizasyon, beş veya altı iş ortağı ve büyük bir danışman popülasyonu muhtemelen farklı seviyelerde uzaktan erişim gerektirir. Çalışanların işten ayrılması ve değişen iş koşulları, uzaktan erişim sunucularından yönetilebilirliğin artmasını da gerektirmektedir; bu, muhtemelen birden fazla güvenlik ilkesini ve erişim kontrolü gereksinimlerini aynı anda yürütmesi gerekecektir.

**Uzaktan Erişim Mekanizmaları**

Uzaktan erişim mimarileri üç genel kategoriye ayrılır: (1) analog modemler ve genel telefon ağı aracılığıyla uzaktan kullanıcı erişimi; (2) ısrarlı veya talep üzerine özel ağ bağlantıları üzerinden erişim; ve (3) İnternet gibi ortak ağ altyapıları yoluyla erişim.

**Telefonlar**

Telefonlar ve analog modemler son yirmi yıldır bilgisayar kaynaklarına uzaktan erişim sağlıyor. Genellikle evde veya otel odasında bulunan bir kullanıcı, bilgisayarını standart bir telefon prizine bağlar ve şirket konumundaki bir ağ erişim sunucusuna (NAS) bir noktadan noktaya bağlantı kurar. NAS, kullanıcı kimlik doğrulaması, erişim kontrolü ve muhasebe işlemlerinin gerçekleştirilmesinden ve telefon bağlantısı canlı iken bağlantıyı sürdürmekten sorumludur. Bu model düşük son kullanıcı maliyetinden yararlanır (telefon ücretleri, yerel aramalar için genellikle çok düşüktür ve genellikle işveren tarafından uzun mesafeli geçiş ücretleri için karşılanır) ve aşinalıktır. Modemler, en azından telefon hatlarına yaygın erişimi olan yerlerde, kullanımı genellikle kolaydır. Modem tabanlı bağlantı, iş yerlerinden uzaktan erişim gerektiğinde daha da sınırlıdır ve bu da kendi tesislerinden esasen sınırsız giden erişimine izin vermek istemeyebilir.

Ancak dezavantajları bol. Tüm telefon sistemleri eşit olarak oluşturulmaz. Eski telefon şebekelerine sahip bölgelerde, elektrik paraziti veya sinyal kaybı, uzak bilgisayarın NAS ile güvenilir bir bağlantı kurmasını engelleyebilir. Bir bağlantı kurulduktan sonra bile, veri aktarım hızı düşükse, bazı ağ uygulamaları (özellikle multimedya paketleri ve ağ gecikmesine duyarlı uygulamalar gibi zamana duyarlı servisler) başarısız olabilir. Bu sorunları şirket karargahlarından çözmek ya da kontrol etmek neredeyse imkansız.

Modem teknolojisi, ekipmanın sık ve potansiyel olarak pahalı bir şekilde bakımını gerektirerek hızla değişmektedir. Ağ erişim sunucuları, düşmanca eylem için popüler hedeflerdir çünkü özel ağa tek bir giriş noktası sağlarlar - çoğunlukla kötü korunan bir ağ geçidi.

**Özel Ağ Bağlantıları**

İş yeri bağlantısı - uzak kurumsal yerler için ağ bağlantıları - ve iş ortağı bağlantıları, özel özel ağ devreleri kullanılarak sık sık karşılanmaktadır. Özel ağ bağlantıları, başlıca telekomünikasyon sağlayıcılarının çoğu tarafından sunulmaktadır. Genellikle birden fazla lokasyona bağlanmanın en güvenli yolu olarak kabul edilirler, çünkü taşıdıkları tek ağ trafiği aynı organizasyona aittir.

Özel ağ bağlantıları iki kategoriye ayrılır: özel devreler ve Frame Relay devreleri. Özel devreler aboneleri için yalıtılmış bir fiziksel devre sağladıkları için en özel olanlardır (dolayısıyla adı).

Özel bir bağlantıdaki tek veri abone kuruluşuna aittir. Saldırgan, yalnızca telekomünikasyon sağlayıcısının kendisine saldırarak özel bir devre altyapısını alt edebilir. Bu önemli bir koruma sunar. Ancak telekom ataklarının korsan sözlükte en eski olanı olduğunu unutmayın - ses hatlarına erişimi kolaylaştıran mekanizmaların çoğu veri devreleri üzerinde de çalışır, çünkü fiziksel altyapı aynıdır. Finansal kurumlar gibi yüksek güvenlikli ortamlar için, özel ağ bağlantılarında bile güçlü kimlik doğrulama ve şifreleme gerekir.

Çerçeve Rölesi bağlantıları, trafiği karelere sığdırarak paylaşılan bir fiziksel altyapı üzerinden özel bant genişliği sağlar. Çerçeve başlığı, trafiği güvenli bir şekilde hedefine ulaştırmak için adresleme bilgilerini içerir. Ancak ortak fiziksel devre kullanımı, özel devrelere göre Çerçeve Rölesi bağlantılarının güvenliğini azaltır. Çerçeve devreleri arasındaki paket sızıntısı iyi bir şekilde belgelenmiştir ve Çerçeve Rölesi devrelerine gizlice giren cihazlar pahalıdır, ancak hazırdır. Bu riskleri azaltmak için birçok satıcı, paket yükünü şifreleyen, kaçaklara ve tıkanmalara karşı koruyan, ancak çerçeve başlıklarını yalnız bırakan, Çerçeve Rölesi özel donanım sağlar.

Özel ağ bağlantılarının güvenliği elbette bir ücretle karşılanıyor - özel bağlantılar için abonelik oranları genellikle İnternet bağlantılarından iki ila beş kat daha yüksek olsa da, yüksek hacimli kullanımlarda indirim önemli olabilir. Eğer telekomünikasyon sağlayıcıları bu alanlarda gerekli ekipmanı sağlayamazsa yalıtılmış alanlara yayılması zordur.

**İnternet Tabanlı Uzaktan Erişim**

Bir kurumsal ağa erişim sağlamanın en uygun maliyetli yolu, mümkün olduğunda ortak ağ altyapısından yararlanmaktır. İnternet her yerde, kullanımı kolay, ucuz bağlantı sağlar. Ancak, önemli ağ güvenilirliği ve güvenlik konularının ele alınması gerekir.

İnternet tabanlı uzaktan kullanıcı bağlantısı ve geniş alan ağları, hem doğrudan ücretlendirme hem de donanım bakım ve destek sistemleri, modern modem bankaları ve özel ağ devrelerinden çok daha ucuzdur. En önemlisi, ISS'ler modemleri ve çevirmeli yönlendirici yöneterek destek yükünü yönlendir ve kurumsal ağ / telekomünikasyon grubundaki yönlendirmeyi yükseltir.

Tabii ki, İnternet üzerinden özel ağ iletişimini güvenceye almak çok önemli bir husustur. Çoğu TCP / IP protokolü, verileri açık metin olarak taşımak ve iletişimi gizlice dinleme saldırılarına karşı savunmasız kılmak üzere tasarlanmıştır. IP kimlik doğrulama mekanizmalarının eksikliği, oturum ele geçirmeyi ve izinsiz veri değiştirmeyi kolaylaştırır (veri aktarılırken). İnternetteki bir şirket varlığı, hizmet reddi saldırılarına özel bilgisayar kaynaklarını açarak sistemin kullanılabilirliğini azaltabilir. Yeni nesil İnternet protokollerinin, özellikle de IPSec'in devam eden gelişimi, bu sorunların çoğuna değinecek. IPSec, paket başına kimlik doğrulama, taşıma yükü doğrulama ve şifreleme mekanizmalarını geleneksel IP'ye ekler. Geniş çapta uygulanıncaya kadar, özel güvenlik sistemleri hassas trafiği bu saldırılara karşı açıkça korumalıdır.

İnternet bağlantısı, özel ağ bağlantılarından çok daha az güvenilir olabilir. İnternet sorunlarını giderme, özellikle de bir kuruluş genel olarak geniş alanlı ağ bağlantılarını kurum içinde yönetmişse, sinir bozucu olabilir. İnternetteki herhangi bir merkezi otoritenin olmayışı, paket kaybı, beklenenden yüksek gecikme süresi ve omurga İnternet sağlayıcıları arasında paket değişimi kaybı gibi hizmet sorunlarının çözülmesi zaman alabilir. Bu kaygının farkına varmakla birlikte, ulusal İnternet servis sağlayıcılarının birçoğu, iş açısından kritik bağlantılar için servis seviyesi anlaşmaları ve geliştirilmiş izleme araçları (daha yüksek maliyetle) sağlayan “business class” İnternet bağlantısı sunmaya başlıyor.

İş gereksinimlerine bağlı olarak, minimum düzeyde bağlantı ve verim düzeyi sağlayacak mekanizmalar göz önüne alındığında, VPN teknolojisi, İnternet tabanlı uzaktan erişim güvenliğini artırmak için kullanılabilir. Bu tartışmanın amaçları doğrultusunda, VPN halka açık bir ağ üzerinden “güvenli bir şekilde iletişim kuran iki veya daha fazla özel sektöre ait ve yönetilen bilgisayar sisteminden oluşan bir gruptur.

Güvenlik özellikleri, uygulamadan uygulamaya kadar farklılık gösterir, ancak çoğu güvenlik uzmanı VPN’lerin, verilerin şifrelenmesini, uzak kullanıcıların ve ana bilgisayarların güçlü şekilde doğrulanmasını ve özel ağ topolojisi hakkındaki bilgileri kamu ağındaki potansiyel saldırganlardan gizlemek veya gizlemek için mekanizmalar içerdiğini kabul eder. İletimdeki veriler, uzaktaki ve kurumsal sunucu arasında şifrelenerek veri gizliliğini ve bütünlüğünü korur. Dijital imzalar verilerin değiştirilmediğini doğrular. Uzaktaki kullanıcılar ve ana bilgisayarlar, bir kerelik şifre üreticileri ve dijital sertifikalar dahil olmak üzere güçlü kimlik doğrulama ve yetkilendirme mekanizmalarına tabidir. Bunlar, yalnızca uygun personelin kurumsal verilere erişebileceğini ve değiştirebileceğini garanti etmeye yardımcı olur. VPN'ler özel ağ adreslerinin genel ağ üzerinden yayılmasını önleyebilir, böylece potansiyel hedef makinelerin hizmet kesintiye uğramaya çalışan saldırganlardan gizlenmesini sağlayabilir.

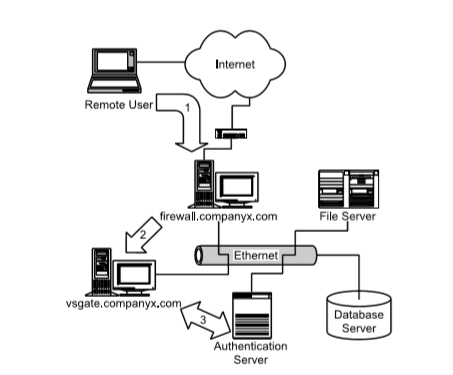


EXHIBIT 9.1 Uzak kullanıcı VPN.

Çoğu durumda, VPN teknolojisi İnternet üzerinden kullanılır, ancak VPN'lerin uzaktan erişim güvenliğini büyük ölçüde artırabileceği başka durumlar da vardır. Bir kuruluşun, iş ortağı konumunda veya müşteri sitesinde çalışan ve özel kampus ağına özel bir özel ağ devresi ile çalışan çalışanları olabilir. Kuruluş, kendi çalışanlarını ev ağlarına geri bağlamak için bir VPN uygulaması kullanmayı seçebilir ve hassas verileri iş ortağı ağında potansiyel olarak dinlenmeye karşı koruyabilir. Genel olarak, özel bir ağ ile örgütün idari veya yönetsel kontrolünün olmadığı bir kuruluş arasında bir bağlantı yapıldığında, VPN teknolojisi, verilerin bozulmasına ve sistem bütünlüğünün kaybına karşı değerli bir koruma sağlar.

Düzgün bir şekilde uygulandığında, VPN'ler, en azından modem tabanlı erişim veya Frame Relay devreleri tarafından sağlananlara eşit granüler erişim kontrolü, hesap verebilirlik, öngörülebilirlik ve sağlamlık sağlar. Çoğu durumda, ağ güvenliği VPN ürünlerinin tasarımında dikkate alındığından, diğer uzaktan erişim teknolojilerinden daha yüksek düzeyde kontrol, denetim yeteneği ve esneklik sağlarlar.

**Uzaktan Erişim Sistemi Seçme**

Küçük, nispeten istikrarlı uzak kullanıcı grupları olan çalışanlar (çalışanlar veya çalışanlar için) olan kuruluşlar için VPN dağıtımının maliyeti, geleneksel uzaktan erişim yöntemlerine göre muhtemelen en düşük düzeydedir.

Bununla birlikte, dinamik kullanıcı toplulukları, karmaşık güvenlik politikaları ve genişleyen iş ortaklıkları için VPN teknolojisi yönetimi basitleştirebilir ve masrafları düşürebilir:

• VPN'ler seyahat eden çalışanların internet üzerinden şirket ağına erişmelerini sağlar. Varsa, uzak sitelerin mevcut İnternet bağlantılarını kullanarak ve bireysel erişim için yerel bir ISS'yi arayarak, pahalı uzun mesafe ücretlerinden kaçınılabilir.

• VPN'ler, müşteri sitelerinde, iş ortaklarında, otellerde ve güvenilmeyen diğer yerlerde çalışan çalışanların, özel ve özel bağlantılar üzerinden bir şirket ağına güvenle erişmelerini sağlar.

• VPN'ler bir kuruluşun İnternet kullanan müşterilere müşteri desteği sunarken, müşterinin bilgisayar ağları için riskleri en aza indirir.

Şirket sunucularına aynı anda birden fazla erişim düzeyinin desteklenmesini gerektiren karmaşık güvenlik ortamları için, VPN'ler idealdir. Çoğu VPN sistemi, geri duvarlar gibi çeşitli çevre güvenlik cihazlarıyla birlikte çalışır. VPN'ler, uzak kullanıcı popülasyonunun yönetimini basitleştiren birçok farklı merkezi kimlik doğrulama ve denetim sunucusunu kullanabilir. Kimlik doğrulama, yetkilendirme ve muhasebe (AAA) sunucuları ayrıca dahili sistemlere ayrıntılı erişim ataması sağlayabilir. Elbette, tüm bu esneklik dikkatli bir tasarım ve test gerektirir - ancak ilk öğrenme eğrisinin faydaları ve uygulama çabası çok büyük.

VPN kullanmanın esnekliği ve maliyet avantajlarına rağmen, bazı durumlarda uygun olmayabilir; Örneğin:

1. VPN'ler, mevcut İnternet bağlantılarını kullanarak maliyetleri düşürür. Uzak kullanıcılar, şirketler şubesi veya iş ortakları İnternete yeterli erişime sahip değilse, bu avantaj kaybedilir.

2. Gerekli uygulamalar SNA veya IPX gibi IP olmayan trafiğe dayanıyorsa, VPN'ler daha karmaşıktır. VPN istemcileri ve sunucuları IP olmayan protokolleri desteklemeli veya IP ağ geçitleri (çeviri aygıtları) tasarıma dahil edilmelidir. Bir ağda ağ geçitlerini sürdürmenin maliyeti ve karmaşıklığı, çeşitli IP dışı iletişimleri destekleyebilecek özel Frame Relay devreleri gibi alternatiflere karşı tartılmalıdır.

3. Bazı endüstrilerde ve bazı kuruluşlarda, İnternet'in özel verilerin iletilmesi için kullanılması yasaktır. Örneğin, federal Sağlık Finansmanı İdaresi, İnternet'in hasta tarafından tanımlanabilen Medicare verilerinin aktarımı için kullanılmasına izin vermez (bu yazı sırasında). Bununla birlikte, özel bir ağ içinde bile, iletimde çok hassas veriler en iyi şekilde şifreleme VPN teknolojisi, özellikle de verilerin toplu olarak şifrelenmesi ve güçlü kimlik doğrulama / dijital sertifikalar kullanılarak korunabilir.

**Uzaktan Erişim Politikası**

Resmi bir güvenlik politikası, uzaktan erişim sorununun çözümünde (ve tüm BT kaynaklarının günlük yönetiminde) tüm teknik, mali ve lojistik kararların hedeflerini ve temel kurallarını belirler. Bilgisayar güvenliği politikaları genellikle bir kuruluşun genel güvenlik çerçevesinin yalnızca bir alt grubunu oluşturur; diğer alanlar arasında çalışanların tespit mekanizmaları, hassas şirket lokasyonlarına ve kaynaklarına erişim, işe alma ve işten çıkarma prosedürleri vb.

Çok az bilgi güvenliği yöneticisi veya denetçisi, kuruluşlarının iyi belgelenmiş bir politikaya sahip olduğuna inanmaktadır. Sözleşmeler, kaynaklar ve yönetici felsefesi öyle değişmektedir ki, güncel belgeleri korumak yasaklayıcı olabilir. Ancak en etkili güvenlik politikaları, şirket içindeki bilgi işlem kaynaklarının kullanımı ve kullanıcıların, operasyon personelinin ve bu bilgisayar sistemindeki yöneticilerin davranışları için beklentileri belirlemektedir. Sistem yöneticileri, yöneticileri ve kuruluş içindeki yasal ve düzenleyici otoriteler üzerinde fikir birliği üzerine kuruludur. En önemlisi, net bir yönetim desteğine sahipler ve çalışan nüfusu boyunca adil ve eşit bir şekilde zorlanıyorlar.

Bir güvenlik politikasının anatomisi şirketten şirkete değişiklik gösterse de, genellikle birkaç bileşen içerir.

• Kesin olarak belirtilen bir amaç tartışılan güvenlik konusunu tanımlar ve dokümanın geri kalanını tanıtır.

• Kapsam, politika için öngörülen izleyici kitlesinin yanı sıra denetim ve uygulama yetkisi zincirini belirtir.

• Giriş politika ve kültürel, teknik ve ekonomik motivasyonları için arka plan bilgisi sağlar.

• Kullanım beklentileri tartışılan kaynağa ilişkin sorumlulukları ve ayrıcalıkları içerir. Bu bölüm kaynağın kurumsal mülkiyetine dair açık bir ifade içermelidir.

• Son bileşen, sistem denetimini ve politikanın ihlal edilmesini kapsar: bir çalışanın kurumsal sistemlerde gizlilik hakkına, devam eden sistem izlemenin uygun şekilde kullanılmasına ve ihlal tespit edildiğinde disiplin cezasına ilişkin açık bir ifade.

Uzaktan erişim bağlamında, kapsamın hangi çalışanların şirket ağına uzaktan erişim için hak kazandığını ele alması gerekir. Yerel ağın “güvenilir” kullanıcısı olan herkese erişim sağlamak cazip gelebilir. Bununla birlikte, uygunsuz erişim riskini en aza indirmeye yardımcı olmak için durum bazında haklı gösterilmeli.

Güvenlik politikası ve uygulama ile ilgili diğer bir önemli konu ise devam eden, son kullanıcı eğitimidir. Uzak kullanıcılar, uzaktan bağlantının uygun kullanımıyla ilgili özel eğitim gerektirir; evlerde, otellerde ve müşteri yerlerindeki bilgisayar güvenliği risklerinin farkında olma; ve uzaktan erişim sistemindeki güvenlik ihlallerinin sonuçları.

**10- Hacker Araçları ve Teknikleri**

Ed Skoudis, CISSP

Son başlıklar, en son hacker araçları ve tekniklerinin bir kurumun hassas bilgisine ve itibarına büyük zarar verebileceğini göstermektedir. Güçlü, kullanımı kolay ve yaygın olarak kullanılan hacker araçlarının yükselişiyle, güvenlik endüstrisindeki birçok kişi bugün hacklemenin altın çağı olduğunu gözlemledi. Bu bölümün amacı, günümüzde yaygın olarak kullanılan bilgisayar ve ağ güvenliğinden ödün vermek için kullanılan araçları tanımlamaktır. Ek olarak, açıklanan her araç ve teknik için, bölüm her saldırı türüne karşı savunma konusunda pratik tavsiyeler sunar.

Bu araçlara ve kullanıcılarına uygulanan terminoloji, özellikle yeraltındaki bilgisayarda bazı tartışmalara neden olmuştur. Geleneksel olarak ve özellikle yeraltındaki bilgisayarda “hacker” terimi, işlerin nasıl yürüdüğünü ve bilgisayar sorunlarına yönelik yenilikçi yaklaşımlar geliştirmeye odaklanan bir kişiye atıfta bulunan iyi huylu bir kelimedir. Bu soylu bireyleri kötü bir saldırgandan ayırt etmek için, bu düşünce okulu kötü niyetli saldırganları “kraker” olarak nitelendiriyor. Bilgisayar korsanları dünyayı daha iyi bir yer haline getirmek için dışarı çıkarken, krakerler hasara ve kargaşaya neden olmak istiyor. Sıklıkla bu terimlerle ilgili karışıklığı önlemek için, bu bölümde, "sistem ve güvenlik yöneticisi" ve "güvenlik uygulayıcısı" terimleri, bu araçları çalıştırmak için meşru ve yetkili bir amacı olan bir kişiyi belirtmek için kullanılacaktır. “Saldırgan” terimi, sistemlere zarar vermek isteyen veya bu tür araçları çalıştırma yetkisi olmayan kişiler için kullanılacaktır.

Bu bölümde açıklanan araçların çoğu çift kişiliklidir; iyilik veya kötülük için kullanılabilirler. Kötü niyetli kişiler tarafından kullanıldığında, araçlar motive olmuş bir saldırganın bir ağa erişmesine, bir uzlaşmanın gerçekleştiği gerçeğini gizlemesine, hatta hizmeti düşürmesine olanak sağlayarak büyük kullanıcı kitlelerini etkiliyor. Güvenlik uygulayıcıları tarafından uygun yetkilendirme ile kullanıldığında, saldırganlardan önce kırılganlıklara karşı “etik saldırı” testleri uygulayarak kendi kuruluşlarının güvenlik duruşlarını ölçmek için bazı araçlar kullanılabilir.

**Uyarı**

Bu bölümün amacı, günümüzde kullanılan çeşitli yeraltı araçlarını açıklamak ve her bir araç türünü ele almak için savunma tekniklerini tartışmaktır. Bu bölüm saldırıları teşvik etmek için tasarlanmamıştır. Ayrıca, aşağıda açıklanan araçlar yalnızca açıklama amaçlıdır ve bu bölümde bahsedilen bir onay değildir. Okuyucular bu araçları denemeye mecbur kalırlarsa, bu araçların sık sık virüslere veya ağlara ve bilgi sistemlerine zarar verebilecek diğer belgelenmemiş özelliklere sahip olduğunu fark ederek kendi riskleri dahilinde yapmaları gerekir. Bu araçları kullanmak isteyen meraklı okuyucular, kaynak kodunu gözden geçirmeli veya hassas üretim sistemlerini korumak için araçları en azından ayrı, hava boşluklu bir ağa kurmalıdır.

**Bilgisayar Yeraltındaki Genel Eğilimler**

Yeraltındaki bilgisayardaki en iyi ve en parlak beyinler, araştırma araştırması yapmak ve günlük olarak yeni güvenlik açıkları ve güçlü, yeni saldırılar bulmaktır. Süper akıllı saldırganlar ve güvenlik uygulayıcıları tarafından yapılan fikirler ve derin araştırmalar yazılım programlarında ve komut dosyalarında uygulanmaktadır. Belirli bir işletim sisteminin kendi şifre şemasını nasıl uyguladığı hakkında aylarca süren araştırmalar kodda işleniyor, bu nedenle ipucu olmayan bir saldırgan (genellikle “script kiddie” olarak adlandırılan) bile yalnızca bir tıkla ve tıkla, çok karmaşık bir saldırı gerçekleştirebiliyor. Senaryo kiddie, araçların gerçek işlevini ve nüanslarını anlamıyor olsa da, saldırının çoğu otomatikleştirildi. Bu ortamda, güvenlik uzmanları, rakiplerinin yeteneklerini hafife almamaya özen göstermelidir. Genellikle, güvenlik ve sistem yöneticileri potansiyel saldırganlarını, interneti gezen basit çocuklar için basit bir av arayanlar olarak düşünürler. Bu değerlendirme bazen doğru olsa da, iki ana kaygısını maskelemektedir. İlk olarak, bu genç çocuklardan bazıları inanılmaz derecede zekidir ve bir ağa zarar verebilir. İkincisi, saldırganlar sadece çocuklar olmayabilir; organize suç, teröristler ve hatta yabancı hükümetler, siber saldırılara sponsorluk yapmakta kaldılar.

**Yüksek Kaliteli Aletlerin Geniş Dağılımı**

Bilişim yeraltındaki bir başka eğilim, araçların yaygın şekilde dağılmasını içerir. Geçmişte (on yıl önce), güçlü saldırı araçları yeraltındaki bilgisayardaki seçkin bir grup elitle sınırlıydı. Bugün, yüzlerce Web sitesi, gezegen üzerindeki her saldırgan (ve güvenlik uygulayıcısı) için araç paylaşımına ayrılmıştır. SSS, her türlü işletim sistemine nasıl girileceğini açıklayan bir programdır. Bu genel eğilimler akıllı saldırganların sistemlerimizin altını oymaya yönelik ayrıntılı bilgi sahibi olduğu bir dünyada birleşirken, o kadar akıllı olmayan saldırganlar gittikçe daha fazla büyüyor. Bu artan tehdidi ele almak için sistem yöneticileri ve güvenlik uygulayıcıları bu araçları ve bunlara karşı nasıl korunacaklarını anlamalıdır. Bu bölümün geri kalanında, günümüzde yaygın kullanımda olan bu çok güçlü araçların birçoğu, bir kişinin ağını her saldırı türünden korumak için pratik savunma ipuçları ile birlikte açıklanmaktadır.

,

**Ağ Haritalama ve Port Tarama**

Bir TCP / IP ağında (İnternet veya şirket intraneti gibi) bir saldırı başlatırken, saldırganın hangi adreslerin etkin olduğunu, ağ topolojisinin nasıl oluşturulduğunu ve hangi hizmetlerin kullanılabilir olduğunu bilmesi gerekir. Bir ağ eşleyici, hedef ağa bağlı sistemleri tanımlar. Bir ağ adres aralığı göz önüne alındığında, ağ eşleyici hangi adreslerin makinelere sahip olduğunu belirlemek için olası her adrese paket gönderir. Bir sunucuya basit bir İnternet Kontrol Mesajı Protokolü (ICMP) paketi göndererek (bir "ping"), eşleme aracı bir sunucunun ağa bağlı olup olmadığını keşfedebilir. Gelen pingleri engelleyen ağlar için, bugün mevcut olan haritalama araçlarının çoğu, bir sunucuya bağlantı kurmayı denemek için tek bir SYN paketi gönderebilir. Bir sunucu dinliyorsa, port açıksa SYN paketi bir ACK'yı ve port kapalı ise potansiyel olarak bir “Port Ulaşılamaz” mesajını tetikler. Bağlantı noktasının açık veya kapalı olmasına bakılmaksızın, yanıt, adresin makine dinlemesine sahip olduğunu gösterir. Bu adres listesiyle bir saldırgan saldırıyı durdurabilir ve bu dinleme sistemlerine odaklanabilir.

Bir port tarayıcı sistemdeki açık portları tanımlar. Bazıları sistemde açık olan, çoğu kapalı olan 65,535 TCP ve 65,535 UDP bağlantı noktası vardır. Ortak hizmetler belirli bağlantı noktalarıyla ilişkilendirilir. Örneğin, TCP Bağlantı Noktası 80, en çok Web sunucuları tarafından kullanılır, TCP Bağlantı Noktası 23, Telnet daemons tarafından kullanılır ve TCP Bağlantı Noktası 25, Internet üzerinden sunucudan sunucuya posta alışverişinde kullanılır. Bir port taraması gerçekleştirerek, bir saldırgan her porta paket gönderir. Temel olarak, portlar bir makinedeki kapılar gibidir. Mevcut binlerce kapıdan birinde ortak servisler dinliyor olacak. Bağlantı noktası tarama aracı, saldırganın kimin cevap verdiğini görmek için bu kapıların her birini vurmasına olanak tanır. Bazı tarama araçları, TCP-baskı özellikleri içerir. İnternet Mühendisliği Görev Gücü (IETF), çeşitli Açıklama İsteklerinde (RFC'ler) TCP ve IP'yi dikkatli bir şekilde belirlese de, tüm paket seçeneklerinin kendisiyle ilişkilendirilmiş standartları yoktur. Sistemlerin yasadışı paket biçimlerine nasıl yanıt vermesi gerektiği konusunda standartlar olmadan, farklı üreticilerin TCP / IP yığınları yasadışı paketlere farklı tepkiler verir. Saldırgan, çeşitli yasadışı paket seçeneklerinin kombinasyonlarını (örneğin bir RST paketiyle bağlantı başlatmak veya diğer garip ve yasadışı TCP kod bitlerini birleştirmek gibi) göndererek, hedef makinede hangi işletim sisteminin çalıştığını belirleyebilir. Örneğin, bir TCP baskı baskısı taraması gerçekleştirerek bir saldırgan, bir makinenin Cisco IOS, Sun Solaris veya Microsoft Windows 2000 kullanıp kullanmadığını belirleyebilir. Bazı durumlarda, bu sürüm kullanılarak belirli bir sürüm veya hizmet paketi seviyesi bile belirlenebilir. Bir saldırgan, ağ haritalama araçlarını ve port tarayıcılarını kullandıktan sonra, hedef ağdaki hangi adreslerin dinleme makinelerine sahip olduğunu, bu makinelerde hangi portların açık olduğunu (ve dolayısıyla hangi servislerin çalıştığını) ve hangi işletim sistemi platformlarının kullanıldığını bilir. Bu bilgi hazinesi, saldırının gerçekleşmesinde saldırganın yararınadır. Bu verilerle, saldırgan erişim sağlamaya çalışmak için belirli hizmetler ve sistemlerdeki güvenlik açıklarını arayabilir. Fyodor tarafından yazılmış Nmap, günümüzde mevcut olan en kapsamlı özellikli haritalama ve tarama araçlarından biridir. Ağ haritalamayı, port taramayı ve TCP yazdırmayı destekleyen Nmap, http://www.insecure adresinde bulunabilir. org / nmap.

**Ağ Haritalama ve Port Tarama Savunmaları**

Ağ eşlemesi ve port taramalarına karşı savunma yapmak için, yönetici tüm gereksiz sistemleri kaldırmalı ve kullanılmayan tüm portları kapatmalıdır. Bunu başarmak için, yönetici gereksiz hizmetleri makineden devre dışı bırakmalı ve kaldırmalıdır. Sadece mutlak, tanımlanmış bir işe sahip olan hizmetler çalışmalıdır. Bir güvenlik yöneticisi, gereksiz bağlantı noktalarının açık olup olmadığını belirlemek için sistemleri düzenli aralıklarla taramalıdır. Keşfedildiğinde, bu gereksiz bağlantı noktaları devre dışı bırakılmalıdır.

**Güvenlik açığı taraması**

Hedef sistemler bir port tarayıcı ve ağ eşleyici ile tanımlandıktan sonra, saldırgan mağdur makinelerde herhangi bir zayıf nokta olup olmadığını belirlemek için arama yapacaktır. Uzaktaki bir saldırganın bir makineye dokunmasını ya da tüm idari kontrolü ele geçirmesini sağlamak için binlerce güvenlik açığı keşfedildi. Bir saldırgan, her güvenlik açığını test etmek için bireysel komutlar girerek her bir sistemde bu güvenlik açıklarının her birini deneyebilir, ancak kapsamlı bir arama yapılması yıllar alabilir. Süreci hızlandırmak için saldırganlar, hedef üzerindeki güvenlik açıklarını hızla aramak için otomatik tarama araçlarını kullanır.

Bu otomatik güvenlik açığı tarama araçları, esas olarak, veritabanını okuyabilen, bir makineye bağlanabilen ve istismara karşı savunmasız olup olmadığını kontrol eden bir motorla iyi bilinen güvenlik açıklarının veritabanlarıdır. Aracın güvenlik açıklarını keşfetmedeki etkinliği, güvenlik açığı veritabanının kalitesine ve eksiksizliğine bağlıdır. Bu nedenle, en iyi güvenlik açığı tarayıcıları, güvenlik açığı veritabanının hızlı bir şekilde yayımlanmasını ve güncelleştirilmesini ve bir komut dosyası dili kullanarak yeni denetimler oluşturma yeteneğini destekler.

Yüksek kaliteli ticari güvenlik açığı tarama araçları yaygın olarak bulunmaktadır ve güvenlik uygulayıcıları ve saldırganlar tarafından güvenlik açıklarını aramak için sıklıkla kullanılır. Ücretsiz cephede, SATAN (Ağı Analiz Etmek İçin Güvenlik Yöneticisi Aracı), 1995 yılında tanıtılan ilk yaygın olarak dağıtılan otomatik güvenlik açığı tarayıcılarından biriydi. Nessus, http: //www.nessus.org. Renaud Deraison tarafından yürütülen Nessus projesi, uzak sistemlerdeki zayıf noktaları tespit etmek için tam özellikli bir tarayıcı sunuyor. Yeni güvenlik açığı kontrolleri yazmak için kaynak kodunu ve bir komut dili içerir ve güvenlik uygulayıcıları ve saldırganlar tarafından özelleştirilmesine olanak tanır.

Nessus, genel amaçlı bir güvenlik açığı tarayıcısı olsa da, çok sayıda sistem ve platformda delik ararken, bazı güvenlik açığı tarayıcıları belirli sistem türlerine daha fazla odaklanır. Örneğin, Whisker, Web sunucusu CGI komut dosyalarına odaklanan tam özellikli bir güvenlik açığı tarama aracıdır. Rain Forest Puppy tarafından yazılan Whisker, http://www.wiretrip.net/rfp adresinde bulunabilir.

**Güvenlik Açığı Tarama Savunmaları**

Yukarıda açıklandığı gibi, yöneticinin kullanılmayan bağlantı noktalarını kapatması gerekir. Ek olarak, sistem güvenlik açıklarının büyük bölümünü ortadan kaldırmak için, sistem yamalarının zamanında uygulanması gerekir. Bilgisayar kullanan tüm kuruluşlar, sistem yamalarının ne zaman ve nasıl güncel tutulacağını belirleyen belirlenmiş bir değişiklik kontrol prosedürüne sahip olmalıdır.

Güvenlik uygulayıcıları ayrıca, saldırganlar yapmadan önce kendi güvenlik ağlarında periyodik güvenlik açığı taraması yapmalıdır. Bu taramalar düzenli olarak (hassas ağlar için üç ayda bir veya hatta aylık olarak) veya büyük ağ değişiklikleri uygulandığında yapılmalıdır. Keşfedilen güvenlik açıkları, sistem yapılandırmalarını güncelleyerek veya yamalar uygulayarak zamanında ele alınmalıdır.

**Wardialing**

Ağ haritalayıcısı ve tarayıcısının kuzeni, bir telefon ağı üzerindeki hedef sistemleri keşfetmek için bir savaş aracıdır. Kuruluşlar, ağlarını güvenlik duvarı, izinsiz giriş algılama sistemi ve güvenli bir DMZ uygulayarak, Internet üzerinden yapılan tam ve ön saldırılardan korumak için büyük miktarda para harcarlar. Ne yazık ki, birçok saldırgan bu rotayı önler ve bunun yerine ağa giden başka yolları arar. Kullanıcıların masaüstünde veya eski, unutulmuş makinelerde bırakılan modemler genellikle bir hedef ağa girmenin en kolay yolunu sağlar.

Aynı zamanda “iblis çeviricileri” olarak da bilinen savaşçılar, kurban ağındaki modemleri bulmaya çalışan bir dizi telefon numarasını çeviriyor. Saldırgan, hedef kuruluşla ilişkili telefon uzantılarını belirleyecektir. Bu bilgiler genellikle telefon rehberini, imza hattındaki telefon iletişim bilgilerini içeren çalışan haber grubu kayıtlarını ve hatta genel çalışan e-postasını listeleyen bir Web sitesinden toplanır. Bir veya bir dizi telefon numarası ile donanmış olan saldırgan, orijinal numara ile ilişkilendirilmiş olan savaş arama aracına girecektir (örneğin, bir haber grubundaki bir çalışanın telefon numarası 555-1212 olarak listelenirse, saldırgan arama yapacak. 555-XXXX). Wardialer, her numarayı otomatik olarak arayacak, bir modem taşıyıcı tonunun tanıdık yoldaşını dinleyecek ve modem dinleyen tüm telefon numaralarının bir listesini yapacaktır.

Saldırganın ürettiği modemlerin listesi ile saldırgan, keşfedilen her modemi bir terminal programı veya başka bir istemci kullanarak arayacaktır. Modeme bağlandıktan sonra, saldırgan afiş bilgilerini temel alarak sistemi tanımlamaya ve bir şifre gerekip gerekmediğine bakmaya çalışacaktır. Genellikle, şifre gerekmez, çünkü modem, saatlerce erişim gerektiren ve onaylanmış yöntemleri kullanarak zahmet etmek istemeyen bir ipucu olmayan kullanıcı tarafından yerine yerleştirilmiştir. Bir şifre gerekirse, saldırgan genellikle platformla veya şirketle ilişkilendirilen şifreleri tahmin etmeye çalışır.

Bazı wardialing araçları ayrıca modemleri tespit etme yeteneğinin yanı sıra tekrarlanan bir çevir sesi bulma özelliğini de destekler. Yinelenen çevir sesi, saldırgan için harika bir şey çünkü bir kurbanın PBX sisteminden dünyanın herhangi bir yerine sınırsız şekilde arama yapabiliyor. Eğer bir saldırgan aynı yerel arama alış verişinde tekrar arama tonunu destekleyen PBX'e bir hat eklerse, saldırgan mağdurun PBX ile kurban tarafından ödenen tüm telefon faturaları ile uluslararası wardialing yapabilir.

Günümüzde mevcut olan en eksiksiz işlevsel wardialing aracı, Hacker’in Seçimi (THC) grubu tarafından dağıtılmaktadır. THC-Scan olarak bilinen bu araç Van Hauser tarafından yazılmıştır ve http://inferno.tusculum.edu/thc adresinde bulunabilir. THC-Scan 2.0, sıralı veya rasgele arama, ağ üzerinden arama, modem taşıyıcı ve tekrar arama tonu algılama ve ilkel algılama önleme yetenekleri gibi birçok gelişmiş özelliği destekler.

**Wardialing Savunmaları**

Wardialing saldırılarına karşı en iyi savunma, belirlenmiş bir iş ihtiyacı olmadan modemlerin ve gelen hatların kullanımını yasaklayan güçlü bir modem politikasıdır. Politika ayrıca, tüm modemlerin bir iş gereksinimi olan merkezi bir veritabanına kaydedilmesini, yalnızca bir güvenlik veya sistem yöneticisi tarafından erişilmesini de gerektirmelidir.

Ek olarak, güvenlik personeli, saldırganlardan önce modemleri bulmak için kendi ağlarının periyodik wardialing egzersizlerini yapmalıdır. Kayıtsız modeme sahip bir telefon numarası bulunduğunda, fiziksel cihaz bulunmalı ve devre dışı bırakılmalıdır. Bu tür aygıtları bulmak zor olsa da, ağ savunucuları saldırganın yapmadan önce bu yenilenen modemleri bulmasına bağlı.

**Ağ Kullanımları: Snifing, Spooing ve Seans Hijacking**

İnterneti oluşturan temel protokol paketi olan TCP / IP, başlangıçta güvenlik hizmeti verecek şekilde tasarlanmamıştır. Aynı şekilde, TCP / IP, Ethernet ile kullanılan en yaygın veri bağlantı tipi temelde güvensizdir. Temel protokollerin bu açıkları göz önüne alındığında, bir dizi saldırı mümkündür.   
Bu ağ açıklarına bağlı olarak en yaygın şekilde kullanılan ve potansiyel olarak zarar verebilecek saldırılar, tehdit, göz atma ve oturum ele geçirmedir.

**Snifting**

Sniffers, bir saldırgan için son derece yararlı bir araçtır ve bu nedenle bir saldırganın araç testinin temel bir unsurudur. Sniffers bir saldırganın ağdan geçen verileri izlemesine izin verir. Ağ trafiğini izleme kabiliyetleri göz önüne alındığında, koklayıcılar, güvenlik pratisyenleri ve ağ yöneticileri için ağ sorunlarını giderme ve araştırmaları yürütmede de faydalıdır. Sniffers, Token Ring ve özellikle Ethernet dahil olmak üzere çeşitli veri bağlantı teknolojilerinin özelliklerinden yararlanır.

En yaygın LAN teknolojisi olan Ethernet, temel olarak bir yayın teknolojisidir. Ethernet LAN'ları hub'lar kullanılarak oluşturulduğunda, LAN'a bağlı tüm makineler LAN segmentindeki tüm verileri izleyebilir. Kullanıcı kimlikleri, şifreler veya diğer hassas bilgiler aynı makinedeki bir makineden (örneğin bir istemci) başka bir makineye (örneğin bir sunucu veya yönlendirici) aynı LAN üzerinden gönderilirse, LAN'a bağlı diğer tüm sistemler verileri izleyebilir. Sniffer, tüm verileri bir LAN segmentinde toplayan bir donanım veya yazılım aracıdır. Bir algılayıcı, sistem tarafından geçen tüm ağ trafiğini toplayan bir makinede çalışırken, Ethernet arayüzünün ve makinenin kendisinin “karışık modda” olduğu söylenir.

Telnet, FTP, POP (e-posta için kullanılan Sonrası Protokolü) ve hatta bazı Web uygulamaları gibi yaygın olarak kullanılan uygulamalar şifrelerini ve hassas verilerini şifreleme olmadan iletir. Bir yayın Ethernet segmentindeki herhangi bir saldırgan, bu şifreleri ve verileri toplamak için bir sniffer kullanabilir.

Bir sistemi ele geçiren saldırganlar, genellikle tehlikeye atılan makineye bir yazılım algılayıcı yüklerler. Bu algılayıcı, saldırgan için bir nöbetçi gibi davranarak, tehlikeye atılan sistem tarafından hareket eden hassas verileri toplar. Sniffer, şifreleri içeren bu verileri toplar ve yerel bir dosyada saklar veya saldırgana iletir. Saldırgan daha sonra bu bilgileri giderek daha fazla sistemi tehlikeye atmak için kullanır. Bir tehlikeye maruz kalmış bir makineye bir sniffer takma, bu makineden geçen verileri toplama ve diğer sistemleri ele geçirmek için sniffed bilgileri kullanma saldırısı metoduna ada atlamalı saldırı denir.

İnternet üzerinde çok sayıda kesme aleti bulunmaktadır. En eksiksiz işlevsel kesme araçları, snift (Brecht Claerhout tarafından http://reptile.rug.ac.be/~coder/snifﬁt/snifﬁt.html adresinde bulunabilir) ve Snort (Martin Roesch tarafından http://www.clark.net/~roesch/security.html). Bazı işletim sistemleri, varsayılan olarak, özellikle Solaris (snoop aracıyla) ve bazı Linux (tcpdump ile birlikte gelen) Linux türleri ile birlikte gelir. Diğer ticari koklayıcılar da çeşitli satıcılardan temin edilebilir.

**Snifing Savunma**

Snifing saldırılarına karşı en iyi savunma, aktarılan verileri şifrelemektir. Parolaları veya diğer hassas verileri açık metin olarak göndermek yerine, uygulama veya ağ verileri şifrelemelidir (SSH, güvenli Telnet vb.).

Koklayıcılara karşı bir diğer savunma Ethernet'in yayın yapısını ortadan kaldırmaktır. LAN oluşturmak için bir hub yerine bir anahtar kullanılarak, bir sniffer ile yapılabilecek hasar sınırlıdır. Bir anahtar, anahtardaki yalnızca gerekli kaynak ve hedef portlar trafiği taşıyacak şekilde yapılandırılabilir. Aynı LAN üzerinde olmasına rağmen, anahtardaki diğer tüm bağlantı noktaları (ve bu bağlantı noktalarına bağlı makineler) bu verileri görmez. Bu nedenle, bir sistemde LAN üzerinde bir tehlike varsa, bu makineye yüklenen bir sniffer, LAN üzerindeki diğer makineler arasında değiş tokuş edilen verileri göremez. Anahtarlar bu nedenle, bir nişancının toplayabileceği verileri en aza indirerek güvenliği arttırmada ve ayrıca ağ performansını iyileştirmeye yardımcı olur.

**IP Spooﬁng**

Başka bir ağ tabanlı saldırı, saldırganı gizlemek ve zayıf kimlik doğrulama yöntemlerinden yararlanmak için bilgisayarın kaynak adresini değiştirmeyi içerir. IP adresi atma, saldırganın saldırı yapmak için başka bir makinenin IP adresini kullanmasına izin verir. Hedef makineler kimlik doğrulaması için IP adresine güveniyorsa, IP taraması sisteme saldırgana erişim verebilir. Ek olarak, IP casusluğu bir saldırganın yakalanmasını çok zorlaştırabilir çünkü günlükler saldırının asıl kaynağını değil, yem adreslerini içerecektir. Bu bölümün diğer bölümlerinde açıklanan araçların çoğu, saldırının gerçek kaynağını gizlemek için IP taramasına dayanır.

**Kaşık Savunması**

Sistemler kimlik doğrulama için IP adreslerini kullanmamalıdır. Kimlik doğrulaması için yalnızca IP adresine dayanan işlevler veya uygulamalar devre dışı bırakılmalı veya değiştirilmelidir. UNIX'de “r-komutları” (rlogin, rsh, rexec ve rcp) bilinen bir şekilde IP casusluk saldırılarına maruz kalmaktadır. UNIX güven ilişkileri, yöneticinin bir şifre sağlamadan r-komutlarını kullanarak sistemleri yönetmesini sağlar. Parola yerine, sistemin IP adresi kimlik doğrulama için kullanılır. Bu büyük zayıflık, r-komutlarını güçlü kimlik doğrulama kullanan yönetim araçlarıyla değiştirmek suretiyle önlenmelidir. Böyle bir araç, güvenli kabuk (ssh), r komutlarının zayıf kimlik doğrulamasını değiştirmek için güçlü şifreleme kullanır. Benzer şekilde, kritik güvenlik ve yönetim fonksiyonları için IP adreslerine dayanan diğer tüm uygulamalar değiştirilmelidir.

Ek olarak, bir kuruluş, çevreyi ağlarına, organizasyonu İnternet'e ve iş ortaklarına bağlayan sızdırma önleyici filtreler yerleştirmelidir. Anti-spoof filtreleri, içeriden geldiğini iddia ederek ağ dışından gelen tüm trafiği azaltır. Bu özellik sayesinde, bu tür filtreler bazı türden saldırı saldırılarını önleyebilir ve tüm çevre ağ yönlendiricilerinde uygulanmalıdır.

**Oturum Çalma**

Engelleme, saldırganın ağ bağlantılarıyla ilgili verileri görüntülemesine izin verirken, bir oturum kaçırma aracı, saldırganın ağ bağlantılarını ele geçirmesine, meşru kullanıcıyı başlatmasına veya bir oturum açmasına izin verir. Oturum ele geçirme araçları, Telnet, rlogin veya FTP gibi kalıcı oturum açma oturumlarına sahip hizmetlere karşı kullanılır. Bu hizmetlerden herhangi biri için bir saldırgan bir oturumu kapatabilir ve çok fazla zarara neden olabilir.

Oturumu ele geçirmeyi gösteren yaygın bir senaryo, bir kullanıcı olan Alice'i, Telnet'i kullanarak başka bir sistemi (Bob) uzaktan yönetmek için giriş yapmış olan bir makineyi içerir. Saldırgan Eve, Alice ve Bob (Alice’in LAN’ı, Bob’un LAN’ı veya Alice’in ile Bob’in LAN'ları arasındaki yönlendiriciler arasında bir ağ segmentinde oturuyor).

Oturumu ele geçirme aracını kullanarak Eve aşağıdakilerden herhangi birini yapabilir:

• Alice’in oturumunu izleyin. Oturum ele geçirme araçlarının çoğu, saldırganların ağda bulunan tüm bağlantıları izlemesine ve hangi bağlantıları kesmek istediklerini seçmelerine izin verir.

• Oturuma komutları ekleyin. Saldırganın Bob'u yapılandırmak için akışa bir veya iki komut eklemesi gerekebilir. Bu tür bir kaçırma olayında, saldırgan hiçbir zaman oturumun kontrolünü tam olarak ele almaz. Bunun yerine, Alice’in Bob’a giriş oturumu, Alice’in yazdığı gibi Bob’da uygulanacak olan çok sayıda komut içerir.

• Oturumu çalın. Çoğu oturum ele geçirme aracının bu özelliği, bir saldırganın oturumu Alice'den alıp doğrudan kontrol etmesini sağlar. Temel olarak, Telnet müşteri kontrolü Bob’un haberi olmadan Alice’ten Eve’e kaydırılıyor.

• Oturumu geri verin. Bazı oturum kaçırma araçları, saldırganın bir oturumu çalmasına, sunucuyla etkileşime girmesine ve ardından oturumu sorunsuz bir şekilde kullanıcıya geri vermesine izin verir. Oturum çalınırken, Alice oturumu kontrol ederken Alice bekletilir. Alice beklemede iken, Alice tarafından yazılan tüm komutlar Eve’in ekranında görüntülenir, ancak Bob’a iletilmez. Havva Bob üzerinde değişiklik yaparak bitirildiğinde, Havva kontrolü Alice'e geri gönderir.

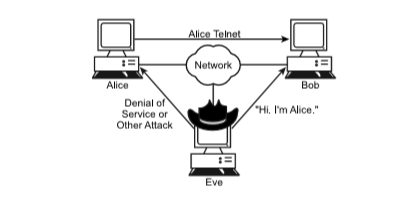


EXHIBIT 10.1 Eve, Alice ile Bob arasındaki seansı kaçırıyor.

Başarılı bir kaçırma olayının gerçekleşmesi için saldırganın Alice ile Bob arasında bir LAN segmentinde olması gerekir. Bir oturum kaçırma aracı, her yöne giden paketlerin TCP sıra numaralarını gözlemleyerek, bir bütünleşik sniffer kullanarak bağlantıyı izler. Alice'ten Bob'a gönderilen her paket, Bob tarafından tüm paketlerin alındığını ve doğru sıralandığını doğrulamak için kullanılan benzersiz bir TCP sıra numarasına sahiptir. Aynı şekilde, Bob’dan Alice’e geri gönderilen tüm paketlerin sıra numaraları vardır. Bir oturum kaçırma aracı, bu sıra numaralarını belirlemek için paketleri koklar. Bir oturum ele geçirildiğinde (komut ekleme ya da oturum çalma yoluyla), ele geçirme aracı otomatik olarak uygun sıra numaralarını kullanır ve Alice'in bıraktığı yerde Bob'la konuşmayı devralarak Alice'in adresini saptar.

Bugün mevcut olan en işlevsel oturum kaçırma araçlarından biri Kra tarafından yazılmış ve http://www.cri.cz/kra/index.html adresinde bulabileceğiniz Hunt. Hunt, bir saldırganın oturumları izlemesini ve çalmasını, tek komutlar eklemesini ve hatta kullanıcıya geri oturum vermesini sağlar.

**Oturum Kaçırma Savunması**

Oturum kaçırmaya karşı en iyi savunma, güvensiz protokollerin ve hassas oturumlar için uygulamaların kullanılmasından kaçınmaktır. Kaçırılması kolay (ve tutması kolay) Telnet uygulamasını kullanmak yerine, daha güvenli, şifreli bir oturum aracı kullanılmalıdır. Saldırganın oturum şifreleme anahtarları olmadığından, şifreli bir oturum kaçırılamaz. Saldırgan basitçe Hunt kullanarak şifreli anlamsız sesler görecek ve yalnızca bağlantıyı sıfırlayabilecek, devralacak ya da komut ekleyemeyecek.

Güvenli kabuk (ssh), Telnet ve rlogin'e oldukça güvenli bir alternatif sağlayan güçlü kimlik doğrulama ve şifreli oturumlar sunar. Ayrıca, ssh, geleneksel FTP'yi değiştirmek için güvenli bir dosya aktarma özelliği (scp) içerir. Güvenli, şifreli Telnet veya kaynak ile hedef arasında kurulan sanal bir özel ağ (VPN) dahil olmak üzere başka alternatifler de mevcuttur.

**Hizmet Reddi Saldırıları**

Hizmet reddi saldırıları bugün mevcut olan en yaygın istismarlar arasındadır. Adından da anlaşılacağı gibi, hizmet reddi saldırısı meşru kullanıcıların bir sisteme erişmesini önler. Birçok kuruluşun can damarı olan ve dünya ekonomisinin büyümekte olan bir parçasını oluşturan E-ticaret uygulamalarıyla, iyi zamanlanmış bir hizmet reddi saldırısı büyük ölçüde hasara neden olabilir. Hassas makineleri veya diğer işlevleri kontrol eden sunucuları aşağı indirerek, bu saldırılar yaşam ve uzuv için gerçek bir fiziksel tehdit oluşturabilir. Saldırgan, sahte trafiği olan bir sistemi silerek veya hatta bilerek sunucunun çökmesine neden olarak hizmet reddine neden olabilir. Sayısız hizmet reddi saldırısı bugün yaygın bir şekilde kullanılıyor ve http://packetstorm.securify.com/exploits/DoS adresinde bulunabilir. En sık kullanılan ağ tabanlı hizmet reddi saldırıları iki kategoriye ayrılır: hatalı biçimlendirilmiş paket saldırıları ve paket saldırıları.

**Kötü Biçimli Paket Saldırıları**

Bu tür bir saldırı genellikle beklenmeyen bir şekilde biçimlendirilmiş bir veya iki paketi içerir. Birçok satıcı ürünü uygulaması, kullanıcı girişlerinin veya paket türlerinin tüm çeşitlemelerini hesaba katmaz. Yazılım bu tür hataları kötü bir şekilde ele alırsa, sistem bu paketleri aldığında çökebilir. Bu tip saldırılara klasik bir örnek, IP fragmanlarının birbiriyle örtüşen bir sisteme gönderilmesini içerir (fragman ofset değerleri yanlış ayarlanmış). Bazı yamalı Windows ve Linux sistemleri bu tür paketlerle karşılaştıklarında çökecektir. Gözyaşı saldırısı, bu IP parçalanma işleme güvenlik açığından yararlanan bir araç örneğidir. TCP / IP uygulamalarında diğer zayıf noktalardan yararlanan diğer hatalı biçimlendirilmiş paket saldırıları arasında rengarenk WinNuke, Land, LaTierra, NewTear, Bonk, Boink vb.

**Paket Taşkın Saldırıları**

Paket servis reddi araçları, ağdaki bir sisteme bir miktar trafik sıkıntısı çekerek meşru kullanıcılara yanıt verme yeteneğini zorluyor. Saldırganlar, en çok SYN'leri olmak, yayın saldırılarını yönlendirmek ve hizmet reddi araçlarını dağıtmakla birlikte bu tür alanları oluşturmak için sayısız teknik geliştirdiler.

SYN araçları, bir dizi SYN paketi göndererek sistemle çok sayıda yarı-açık bağlantı başlatır. Herhangi bir TCP bağlantısı kurulduğunda, üç yönlü bir el sıkışma meydana gelir. Başlangıç ​​sistemi (genellikle müşteri), o oturumdaki kaynaktan hedefe giden tüm paketler için bir sıra numarası oluşturmak üzere hedefe bir SYN paketi gönderir. Hedef, kaynaktan hedefe giden paketler için dizi numarasını onaylayan ve karşı yöne giden paketler için bir ilk dizi numarası belirleyen bir SYN-ACK paketi ile yanıt verir. Kaynak, hedefe bir ACK göndererek üç yönlü el sıkışmasını tamamlar. Üç yollu el sıkışma tamamlandı ve iletişim (gerçek veri aktarımı) gerçekleşebilir.

SYN ’ler TCP’nin üç yollu el sıkışmasında zayıflıktan yararlanıyor. Saldırgan, yalnızca sahte SYN paketleri göndererek ve hiçbir zaman SYN-ACK'ya yanıt vermediğinde, sunucunun başlatılan tüm oturumların durumunu koruma yeteneğini tüketebilir. Çok sayıda yarı açık bağlantı adı verilen bir sunucu ile bir sunucu yeni, meşru bir trafiği kaldıramaz. Tüm boru bant genişliğini bir sunucuya bağlamak yerine, yalnızca sunucunun oturum başlatma işlemlerini gerçekleştirme kapasitesinin aşırı boğulması gerekir (çoğu ağ konfigürasyonunda, bir sunucunun SYN'leri işleme yeteneği sitenin toplam bant genişliğinden düşüktür). Bu nedenle, SYN od ooding en popüler paket saldırısıdır. ICMP ve UDP paketlerine sahip sistemleri kullanan diğer araçlar da mevcuttur, ancak bunlar sadece bant genişliği kullanırlar, bu nedenle bir saldırgan tüm hizmetleri kesmek için kurbandan daha büyük bir bağlantıya ihtiyaç duyar.

Saldırganların bant genişliğini artırmalarına izin veren başka bir paket türü, yönlendirilmiş yayın saldırısıdır. Genelde, bu tekniği kullanan ilk araçtan sonra adlandırılan bir saldırı saldırısı olarak adlandırılan yayın saldırıları, üçüncü tarafın ağını paketin elçisi olarak kullandı. Bir saldırı saldırısında, saldırgan Internet'te yayın ICMP iletisine yanıt verecek bir ağ bulur (esas olarak ağın yayın adresine ping). Ağ, yayın isteklerine ve yanıtlarına izin verecek şekilde yapılandırılmışsa, ağdaki tüm makineler ping'e bir yanıt gönderir. ICMP isteğini yerine getirerek, saldırganın üçüncü taraf ağdaki tüm makinelerin mağdurlara yanıt göndermesini sağlayabilirsiniz. Örneğin, bir kuruluşun İnternete bağlı tek bir DMZ ağında 30 ana bilgisayarı varsa, bir saldırgan, DMZ'ye ping gönderen sahtekar bir ağ gönderebilir. Her 30 ev sahibi, nihai kurban olacak sahte adrese bir yanıt gönderecek. Saldırganın tekrar tekrar gönderdiği mesajlar gönderildiğinde, saldırganın 30 kat fazla bant genişliği vardır. Yalnızca 56 kbps çevirmeli ağ hattına sahip bir saldırgan bile bu seviyedeki bir T1 hattını (1,54 Mbps) oluşturabilir. Diğer yönlendirilmiş yayın saldırı araçları arasında Fraggle ve Papasmurf bulunur.

Önemli bir baskı alan son hizmet reddi türü, hizmet reddi saldırısıdır. Temel olarak standart paket kavramlarına dayanan Şubat 2000'de birçok büyük İnternet sitesini engellemek için hizmet reddi saldırıları kullanıldı. Trin00, Tribe Flood Network 2000 (TFN2K) ve Stacheldraht gibi araçlar bu tür saldırıları destekliyor. Dağıtılmış hizmet reddi saldırısı yapmak için, saldırganın İnternet üzerinde çok sayıda savunmasız sistem bulması gerekir. Genellikle, bir düzine, yüz hatta binlerce makineyi devralmak için aşırı akış saldırısı (aşağıda açıklanmıştır) gibi uzak bir tampon kullanılır. Saldırgan tarafından ele geçirilen bu makinelere zombiler adı verilen basit daemon işlemleri yüklenmiştir. Saldırgan, bir kontrol programı kullanarak bu zombi ağı ile iletişim kurar. Kontrol programı, yüzlerce veya binlerce zombiye komut göndermek ve eşzamanlı olarak aynı işlemi yapmalarını istemek için kullanılır.

Alınacak en yaygın eylem, aynı anda bir hedefe karşı bir paket unu başlatmaktır. Geleneksel bir SYN, bir ana bilgisayardan gelen paketleri içeren bir hedefi engellerken, dağıtılmış bir hizmet reddi saldırısı, çok yüksek bant genişliğine sahip, iyi tasarlanmış sitelerin kapasitesini hızla tüketen çok sayıda zombiden paketler gönderir. Dağıtılmış hizmet reddi saldırı araçlarının çoğu, SYN, UDP ve ICMP'nin kokusu, şirin saldırıları ve bazı hatalı biçimlendirilmiş paket saldırılarını destekler. Bu seçeneklerden herhangi biri veya tümü, kontrol programı kullanılarak saldırgan tarafından seçilebilir.

**Hizmet Reddi Saldırı Savunması**

Hatalı biçimlendirilmiş paket saldırılarına karşı korunmak için sistem yamaları ve güvenlik dosyalarının düzenli olarak uygulanması gerekir. Satıcılar, hizmet reddi saldırısının yeni alanını ele almak için sistemlerini sık sık yamalar ile günceller. Bir kuruluşun, güvenlik sertifikaları için satıcı ve endüstri güvenlik bültenlerini izlemek için bir programa ve açıklanmaları ve test edilmelerinden hemen sonra bu ilaçları uygulamak için kontrollü bir metoda sahip olması gerekir.

Paket kaynaklı saldırılar için kritik sistemler, tek bir başarısızlık noktasını ortadan kaldırarak birden fazla, gereksiz yolu olan temel ağ mimarilerine sahip olmalıdır. Ayrıca, yeterli bant genişliği şarttır. Ayrıca, bazı yönlendiriciler ve geri dönüş duvarları bir SYN yükünün yükünü hafifletmek için trafik kontrolünü desteklemektedir.

Son olarak, internete erişilebilen bir ağın uygun şekilde yapılandırılmasıyla bir kuruluş, bunun şirin ve dağıtılmış hizmet reddi saldırıları için bir başlangıç ​​noktası olarak kullanılması olasılığını en aza indirebilir.

Şirin olarak kullanılma olasılığını önlemek için, tüm yönlendirilmiş yayın taleplerini İnternet'ten düşürmek için dış yönlendirici veya güvenlik duvarı yapılandırılmalıdır. Dağıtılmış bir hizmet reddi saldırısında kullanılma şansını azaltmak için bir kuruluşun, dışarıdan gelen tüm trafiğin sitenin kaynak IP adresine sahip olduğundan emin olmak için dış yönlendiriciler ve geri dönüş duvarları üzerine anti-spoof filtreleri uygulaması gerekir. Bu çıkış filtreleme, saldırganın ağda bulunan bir zombi veya hizmet reddi aracından sahte paket göndermesini önler. İnternetten gelen tüm paketleri, birinin dahili ağından geldiğini iddia eden antispoof giriş filtreleri, hizmet reddi saldırılarını önlemede de faydalıdır.

**Yığın Tabanlı Tampon Aşırı Yük**

Yığın tabanlı aktarma saldırıları yığın saldırgan tarafından ağ üzerinden uzaktan bir sistemi ele geçirmek için yaygın olarak kullanılır. Ek olarak, satırlar üzerindeki arabellek, yerel kötü niyetli kullanıcılar tarafından ayrıcalıklarını yükseltmek ve bir sisteme süper kullanıcı erişimi sağlamak için kullanılabilir. Yığın tabanlı tampon üzerinden akış saldırıları, birçok işletim sisteminin yığınlarını işleme biçiminden, programları çalıştırarak geçici olarak veri depolamak için kullanılan dahili bir veri yapısından yararlanır. Bir işlev çağrısı yapıldığında, yürütme programının mevcut durumu ve işleve iletilecek değişkenler yığına itilir. İşlev tarafından kullanılan yeni yerel değişkenler de yığında boşluk tahsis edilir. Ek olarak, yığın işlevi çağıran kodun dönüş adresini saklar. Bu geri dönüş adresine, işlev çağrısı tamamlandıktan sonra yığından erişilir. Sistem bu adresi çağıran programın yürütülmesini uygun bir yerde sürdürmek için kullanır. Sergi 10.2 bir yığının nasıl yapıldığını gösterir.

Çoğu UNIX ve tüm Windows sistemleri, verileri ve yürütülebilir kodları tutabilecek bir yığına sahiptir. Bir işlev çağrıldığında yerel değişkenler yığında depolandığından, bu değişkenlerin sınırlarını üst üste koymak için zayıf koddan yararlanılabilir. Eğer kullanıcı girişi uzunluğu kodla incelenmezse, yığın üzerindeki belirli bir değişken, yığın üzerinde kendisine ayrılan hafızayı aşabilir, tüm değişkenlerin üzerine yazabilir ve fonksiyon tamamlandıktan sonra yürütmenin devam etmesi gereken dönüş adresleri bile olabilir. Yığın "parçalanması" olarak adlandırılan bu işlem, bir saldırganın, yerel değişkenleri çalıştırılabilir kod ve yığına başka bir dönüş adresi eklemek için devretmesine izin verir. Sergi 10.2 ayrıca, aşağıya bir tampon ile parçalanmış bir yığını gösterir.

Saldırgan, çalıştırılabilir komutlardan oluşan (genellikle bir kabuk rutini) makineye özgü bayt kodları ve bu eklenen komutların yürütülmesini başlatmak için bir dönüş işaretçisiyle yığındaki tamponu yükler. Bu nedenle, çok dikkatli bir şekilde oluşturulmuş ikili kodla, saldırgan kullanıcı olarak gerçekten yürütülebilir kod ve yeni bir dönüş adresinden oluşan bir programa bilgi girebilir. Adamcağız program bu girişin uzunluğunu analiz etmeyecek, ancak yığına yerleştirecek ve saldırganın kodunu çalıştırmaya başlayacaktır. Bu güvenlik açıkları bir saldırganın uygulama kodundan çıkmasına ve bozuk programın izinleriyle sistem bileşenlerine erişmesine izin verir. Bozuk program süper kullanıcı ayrıcalıklarıyla çalışıyorsa (örn., Bir UNIX sistemindeki SUID kökü), saldırgan, makinenin üzerinden bir arabellek kullanarak makineyi devraldı.

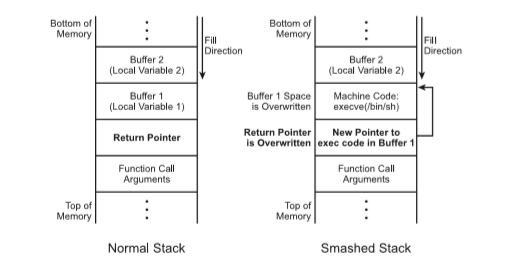


EXHIBIT 10.2 Normal bir yığın ve üzerinde bir arabellek bulunan bir yığın.

**Yığın Tabanlı Tampon Aşırı Yük Savunması**

Arabellek aşırı yük saldırılarına karşı en kapsamlı savunma yazılımı düzgün bir şekilde kodlamaktır, böylece yığını parçalamak için kullanılamaz. Tüm programlar, kullanıcılardan ve diğer programlardan gelen tüm girdileri doğrulamalı ve ayrılan bellek yapılarına girmesini sağlamalıdır. Her bir değişken kontrol edilmeli (kullanıcı girişi, diğer fonksiyonlardan değişkenler, diğer programlardan giriş ve hatta ortam değişkenleri dahil), atanan tamponların verileri tutmak için yeterli olduğundan emin olmak için. Ne yazık ki, bu nihai çözüm yalnızca programları yazan ve kaynak kodu olan kişiler için geçerlidir.

Ek olarak, güvenlik pratisyenleri ve sistem yöneticileri, kullanıcıların çalıştırabileceği ve diğer kullanıcıların (root gibi) izinlerine sahip olabilecekleri bir sistemdeki SUID programlarının sayısını dikkatlice kontrol etmeli ve en aza indirmelidir. Hassas sistemlere yalnızca açık bir iş gereksinimi olan SUID programları yüklenmelidir.

Son olarak, birçok yığın tabanlı arabellek taşma saldırısı, sistemleri yığından kod çalıştırmamaya zorlayarak önyüklenebilir. Özellikle, Solaris ve Linux bu seçeneği sunar. Örneğin, Solaris sistemini yığın tabanlı arabelleklere karşı aşılamak için, aşağıdaki satırlar eklenmelidir:

/etc/system:

set noexec\_user\_stack=1 set noexec\_user\_stack\_log=1

İlk satır bir istif üzerinde çalışmayı önler ve ikinci satır herhangi bir girişimi kaydeder. Ne yazık ki, bazı programlar yasal olarak yığından kod çalıştırmaya çalışır. Bu seçenek uygulanırsa bu programlar çökecektir. Genel olarak, sistem tek bir amaç ise ve güvenli olması gerekiyorsa (örneğin bir Web sunucusu), bu seçenek yığın tabanlı arabellek akışını önlemek için kullanılmalıdır.

**Parola Kırma Sanatı ve Bilimi**

Günümüzde sistemlerin büyük çoğunluğu, kullanıcıları statik bir parola ile doğrulamaktadır. Bir kullanıcı oturum açtığında, sisteme şifre gönderilir ve bu, kullanıcının giriş yapmasına izin verip vermemeye karar vermek için şifreyi kontrol eder. Bu kararı verebilmek için sistemin, kullanıcının girişini gerçek şifre ile karşılaştıracak bir mekanizmasına sahip olması gerekir. . Elbette, sistem sadece tüm şifreleri yerel olarak depolayabilir ve bu dosyadan karşılaştırabilir. Bununla birlikte, bu tür bir açık metin şifresi, bir saldırgan için çok sulu bir hedef sağlayacaktır. Hedefi saldırganlar için daha az kullanışlı hale getirmek için, çoğu modern işletim sistemi saklanan şifreleri korumak için tek yönlü bir karma veya şifreleme mekanizması kullanır. Bir kullanıcı bir parola yazdığında, sistem kullanıcının girişini sağlar ve bunu saklanan karma ile karşılaştırır. İki karma eşleşirse, şifre doğrudur ve kullanıcı giriş yapabilir.

Parola kırma araçları, bu parola koruma yöntemine saldırmak için kullanılır. Bir saldırgan şifreli veya şifreli şifreyi bir sistemden toplamak için bazı istismarlar (genellikle üzerlerinde bir tampon) kullanır (şifre gölgelemeden bir UNIX sisteminde, herhangi bir kullanıcı şifreli şifreyi okuyabilir). Şifreli şifreyi indirdikten sonra, saldırgan kullanıcıların şifrelerini belirlemek için bir şifre kırma aracı kullanır. Kırma aracı bir döngü kullanarak çalışır: bir parola tahmin eder, parolayı özetler veya şifreler ve çalınan alandaki karma parola ile karşılaştırır. Karma eşleşirse, saldırganın şifresi vardır. Karma eşleşmiyorsa, döngü başka bir şifre tahminiyle tekrar başlar.

Parola kırma araçları, parola tahminlerini bir sözlük veya tam bir kaba kuvvet saldırısına dayanarak her olası parolayı dener. İngilizce, Fransızca, Almanca, Klingon, vb. Birçok dilde online olarak sözlükler mevcuttur.

Çok sayıda şifre kırma aracı mevcut. En popüler ve tam işlevli şifre kırıcılar şunlardır:

• Solar Designer tarafından hazırlanan Ripper John, UNIX şifrelerini kırmaya odaklanıyor ve

http: // www.openwall.com/john/ adresinde bulunabilir.

• Windows NT şifrelerini kırmak için kullanılan L0phtCrack, http://www.l0pht.com adresinde bulunabilir.

**Şifre Kırma Savunması**

Parola kırmaya karşı ilk savunma, şifreli / şifreli parolanın maruz kalmasını en aza indirmekten. UNIX sistemlerinde, sadece süper şifreli şifreyi okuyor. Windows NT sistemlerinde, NT 4.0 SP3 ve sonraki sürümlerinde bulunan SYSKEY özelliği mevcut ve etkin durumda. Ayrıca, tüm yedeklemeler ve sistem güvenliği diskleri fiziksel olarak güvenlidir saklanmalı ve hatta şifrelenmiştir.

Güvenli bir şifre politikası, güvenli bir ağın sağlanmasında çok önemli bir unsurdur. Bir şifre politikası, sekiz karakterden daha uzun şifre uzunlukları, her şifrede alfanümerik ve özel karakterlerin kullanılmasını gerektirir ve kullanıcıları karma harfli şifrelere sahip olmaya zorlar. Kullanıcıların zayıf şifreler sorununun farkında olmaları ve akılda kalıcı ancak farklı tahmin edilebilecek şifreler oluşturma konusunda eğitilmeleri gerekir.

Parolaların güvenli olmasını sağlamak ve zayıf parolaları belirlemek için, güvenlik uzmanları parola kırma araçları kullanarak sistem parolalarını düzenli aralıklarla denetlemelidir. Zayıf şifreler keşfedildiğinde, güvenlik grubu, şifreleri kolayca tahmin edilebilecek kullanıcılarla etkileşime geçmek için belirlenmiş bir prosedür olmalıdır.

Son olarak, kullanıcıların şifrelerini kolayca tahmin edilebilecek değerlere ayarlamasını önleyen çeşitli yazılım paketleri mevcuttur. Bir kullanıcı yeni bir şifre belirlediğinde, bu filtreleme programları tamamen karmaşık olduğundan emin olmak için şifreyi kontrol eder ve sadece kullanıcı adının veya sözlük kelimesinin bir çeşitlemesi değildir. Bu tür bir araçla, kullanıcılar kolayca önemli bir güvenlik sorununu ortadan kaldıran, kolayca tahmin edilebilecek şifreler oluşturamazlar. Filtreleme yazılımının etkili olması için, kullanıcıların UNIX sunucuları, Windows NT Birincil ve Yedek Etki Alanı Denetleyicileri ve Novell sunucuları dahil olmak üzere şifreler oluşturduğu tüm sunuculara kurulmaları gerekir.

**Arka kapılar**

Arka kapılar, sistemdeki geleneksel güvenlik kontrollerini atlayan, saldırganın bir sistem şifresi sağlamadan ve giriş yapmadan makineye erişmesini sağlayan programlardır. Saldırganlar, daha sonra sisteme erişebilmelerini sağlamak için makineye arkaya monte eder (veya kullanıcıyı kendilerine takmaya zorlar). Kurulduktan sonra, çoğu arka kapı saldırgandan ağ üzerinden gelen bağlantılar için özel bağlantı noktalarını dinler. Saldırgan arka kapı dinleyicisine bağlandığında, geleneksel kullanıcı kimliği ve parola ya da diğer kimlik doğrulama biçimleri atlanır. Bunun yerine, saldırgan şifre girmeden veya yalnızca arka kapıya girmek için kullanılan özel bir şifre kullanarak sisteme erişebilir.

Netcat, Hobbit tarafından UNIX ve Weld Pond tarafından Windows NT için yazılmış inanılmaz esnek bir araçtır (her iki sürüm de http: // www. L0pht.com/~weld/netcat/ adresinde bulunabilir). Çok sayıdaki diğer kullanımları arasında, Netcat, herhangi bir TCP veya UDP bağlantı noktasında süper kullanıcı düzeyinde bir kabuğa sahip bir arka kapı dinleyicisi oluşturmak için kullanılabilir. Windows sistemlerinde, Back Oriﬁce 2000 (kısa olarak BO2K olarak adlandırılan ve http://www.bo2k.com adresinde bulunabilir) ve http://www.bo2k.com adresinde bulunabilir) dahil olmak üzere çok sayıda arka kapı uygulaması mevcuttur. http://www.hack-atack.com).

**Arka kapı savunması**

Arka kapı programlarına karşı en iyi savunma, sistem ve güvenlik yöneticilerinin makinelerinde nelerin çalıştığını bilmesi, özellikle kritik bilgileri depolayan veya yüksek değerli işlemleri gerçekleştiren hassas sistemlerdir. Birdenbire bağlantı noktasını dinleyen süper kullanıcı olarak çalışan bir işlem görüldüğünde yöneticinin araştırması gerekir. UNIX ve Windows NT sistemlerinde netstat –na komutunu kullanarak çeşitli portlarda dinleyen arka kapılar keşfedilebilir.

Ek olarak, birçok arka kapı programı (BO2K gibi), tüm kullanıcıların masaüstlerine ve bir kuruluştaki sunuculara yüklenmesi gereken bir virüsten koruma programı tarafından keşfedilebilir.

**Truva Atları ve Kök Kitleri**

Saldırganın en büyük aracının en önemli unsurlarından biri Truva atı programıdır. Antik Yunanistan'ın Truva atı gibi, bu yeni Truva atlarının da bazı yararlı işlevleri var gibi görünmektedir, ancak gerçekte bazı kötü niyetli faaliyetleri gizlemektedir. Örneğin, bir kullanıcı elektronik posta ile çalıştırılabilir bir doğum günü kartı programı alabilir. Şüpheli olmayan kullanıcı doğum günü kartı programını etkinleştirdiğinde ve doğum günü pastalarının ekran boyunca dans etmesini izlerken, program gizlice bir arka kapı kurar veya kullanıcıların sabit diskini siler. Bu örnekte gösterildiği gibi, Truva atları aldatmacaya güveniyorlar - bir kullanıcıyı veya sistem yöneticisini (görünür) kullanışlılıkları için çalıştırmaları için kandırıyorlar, ancak asıl amacı kullanıcının makinesine saldırmak.

**Geleneksel Truva Atları**

Geleneksel bir Truva atı sadece bir kullanıcı veya yönetici tarafından çalıştırılabilen bağımsız bir programdır. Aşağıdakiler de dahil olmak üzere sayısız geleneksel Truva atı programı geliştirilmiştir:

• Bilinen doğum günü kartı veya tatil tebrik e-posta eki yukarıda açıklanmıştır.

• Bir CD-ROM okuyucularını CD yazma aygıtlarına dönüştürebildiğini iddia eden yazılım programı. Her ne kadar bu başarının yazılımda gerçekleştirilmesi imkansız olsa da, birçok kullanıcı bu "aracı" nı indirmeye başladı.

• Bir Güvenlik açığı tarayıcı, WinSATAN. Bu araç, bir Windows NT sistemi kullanan sistem ve güvenlik yöneticileri için uygun bir güvenlik açığı taraması sağladığını iddia ediyor. Ne yazık ki, bu programı çalıştıran şüphesiz bir kullanıcı da silinmiş bir sabit sürücüye sahip olacaktır.

Sayısız başka örnekler var. Kavramsal olarak çekici olmasa da, kullanıcılar dikkatli olmazsa ve makinelerinde güvenilmeyen programlar çalıştırırsa geleneksel Truva atları büyük bir sorun olabilir.

**Rootkitleri**

Bir RootKit, bir Truva atı kavramını çok daha güçlü bir seviyeye taşır. Ad başka türlü ima etse de, RootKits bir saldırganın bir sisteme "root" (süper kullanıcı) erişimi kazanmasına izin vermez. Bunun yerine, RootKits, zaten bir yönetici tarafından işgalin tespitini denemek için tüm girişimleri engelleyerek bu erişimi korumak için zaten süper kullanıcı erişimine sahip bir saldırgana izin verir. RootKits, kritik sistem programlarını değiştiren veya yama alan tüm Truva atı programlarından oluşur. Yöneticilerin makinelerindeki saldırganları tespit etmek için kullandıkları çeşitli araçlar RootKits ile rutin olarak baltalanır.

Çoğu RootKits, bir Truva atı arka kapı programı içerir (UNIX'te / bin / login yordamı). Saldırgan, önceki sürümün üzerine yazarak / bin / login adında yeni bir Truva atı sürümü yükleyecektir. RootKit / bin / login rutini, saldırganın sisteme daha sonra erişebilmesi için özel bir arka kapı kullanıcı kimliği ve şifresi içerir.

Ek olarak, RootKits bir sniffer ve snifferin gizlenmesi için bir program içerir. Yönetici ifcon komutunu çalıştırarak sistemdeki bir algılayıcıyı algılayabilir. Eğer bir sniffer çalışıyorsa, ifcon çıkışı PROMISC contain ag içerecektir, bunun anlamı Ethernet kartının proiscu modda olduğunu ve bu nedenle de bittiğini gösterir. RootKit, bir saldırganın tespit edilmesini önleyen, PROMISC jan ag göstermeyen bir ifcon Tro g Truva atı sürümü içerir.

UNIX tabanlı RootKits ayrıca ps ve du dahil olmak üzere diğer kritik sistem çalıştırılabilirlerinin yerini alıyor. Hangi işlemlerin çalıştığını belirlemek için kullanıcılar ve yöneticiler tarafından verilen ps komutu, bir saldırganın işlemleri gizleyebilmesi için değiştirilir. Disk kullanımını gösteren du komutu, RootKit ve saldırganın diğer programlarının kapladığı alanın maskelenebilmesi için değiştirildi.

/ Bin / login, ifcon ps g, ps, du ve diğerleri gibi programları değiştirerek, bu RootKit araçları işletim sisteminin kendisinin bir parçası haline gelir. Bu nedenle RootKits, bir yöneticinin gözlerini ve kulaklarını kapatmak için kullanılır. Bilgisayarda sistem yöneticisine iyi görünen sanal bir dünya yaratırlar; gerçekte bir saldırgan oturum açabilir ve cezasız bir şekilde sistemde dolaşabilir. RootKits, çoğu UNIX sistemi ve Windows NT için geliştirilmiştir. Çok çeşitli UNIX RootKits http://packetstorm.securify.com/UNIX/penetration/rootkits adresinde bulunurken, NT RootKit http://www.rootkit.com adresinde bulunabilir.

Bu alanda son zamanlardaki bir gelişme, çekirdek düzeyinde RootKits’in piyasaya sürülmesidir. Bu RootKits, bir işletim sisteminin en temel seviyelerinde hareket eder. / Bin / login ve ifcon application g gibi uygulama programlarını değiştirmek yerine, çekirdek seviyesindeki RootKits aslında sisteme çok düşük seviyeli erişim sağlamak için çekirdeği yatar. Bu araçlar, Linux ve Solaris dahil olmak üzere birçok yeni UNIX varyantının desteklediği yüklenebilir çekirdek modüllerine dayanmaktadır. Yüklenebilir çekirdek modülleri, bir yöneticinin sistemi yeniden başlatmadan bile çekirdeğe işlevsellik eklemesini sağlar. Süper kullanıcı erişimine sahip bir saldırgan, programların yürütülmesine yeniden izin verecek bir çekirdek düzeyinde RootKit yükleyebilir.

Bir yönetici bir programı çalıştırmaya çalıştığında, Truva atı çekirdeği, yürütme isteğini saldırganın programına gönderir; bu, erişim veya başka bir Truva atı sunan bir arka kapı olabilir. Çekirdek yürütme isteklerinin yeniden yapılmasını sağladığından, bu tür bir etkinliği tespit etmek çok güçtür. Yönetici yeniden ele geçirilen dosyaya bakmaya veya bütünlüğünü kontrol etmeye çalışırsa, programın görüntüsü değiştirilmediğinden program değişmemiş görünecektir. Bununla birlikte, yürütüldüğünde, değiştirilmemiş program atlanır ve kötü niyetli bir program çekirdek yerine kullanılır. Creed tarafından yazılan Knark, http://packetstorm.securify.com/UNIX/penetration/rootkits adresinde bulunabilen bir çekirdek düzeyinde RootKit'dir.

**Truva Atları ve KökKit Savunması**

Geleneksel Truva atlarına karşı korunmak için kullanıcı bilinci çok önemlidir. Kullanıcılar, güvenilmeyen programları indirme ve bunları çalıştırma ile ilgili riskleri anlamalıdır. Ayrıca, güvenilir olmayan kaynaklardan gelen e-postalarda çalıştırılabilir eklerin çalıştırılmasının sorunlarından haberdar olmaları gerekir.

Ek olarak, bazı geleneksel Truva atları virüsten koruma programları tarafından algılanabilir ve ortadan kaldırılabilir. Her son kullanıcı bilgisayar sistemi (ve hatta sunucuları) etkin ve güncel bir anti-virüs programına sahip olmalıdır.

RootKits'e karşı savunmak için, sistem ve güvenlik yöneticileri kritik sistem dosyaları için bütünlük kontrol programlarını kullanmalıdır. Bir RootKit kurulduğunda sıkça değiştirilen çalıştırılabilir kodlardan oluşan saygın Tripwire da dahil olmak üzere çok sayıda araç bulunmaktadır. Yönetici bu hash'leri korumalı bir ortama (yazmaya karşı korumalı bir disk gibi) saklamalı ve makinedeki programların doğruluğunu korumalı hashelerle periyodik olarak kontrol etmelidir. Genellikle, bu kontrol türü makinenin hassasiyetine bağlı olarak en az haftada bir yapılır. Yönetici, bu kritik sistem dosyalarında tespit edilen değişiklikleri son yamalar ile bağdaştırmalıdır. Sistem dosyaları değiştirilmişse ve yönetici tarafından herhangi bir yama yüklenmemişse, kötü niyetli bir kullanıcı veya dış saldırgan bir RootKit kurmuş olabilir. Bir RootKit algılanırsa, tamamen kaldırılmasını sağlamanın en güvenli yolu tüm işletim sistemini ve hatta kritik uygulamaları yeniden kurmaktır.

Ne yazık ki, çekirdek düzeyinde RootKits bütünlük kontrol programlarıyla algılanamaz, burada bütünlük denetleyicisi işin hedefi için temel çekirdeğe güvenir. Çekirdek bütünlük denetleyicisine bakıyorsa, sonuçları RootKit kurulumunu göstermez. Çekirdek düzeyindeki RootKit'e karşı en iyi savunma, yüklenebilir çekirdek modüllerini desteklemeyen monolitik bir çekirdek. Kritik sistemlerde (Internet, İnternet Web Sitesi, DNS İnternet, Posta Servisi vb.) Yöneticiler, yüklenebilir çekirdek modüllerini desteklemeden sistemleri tam çekirdek sistemlerle kurudur. Bu özellik ile, sistem bir saldırganın kök dizinini ayarlama kazanmasını ve çekirdeği gerçek zamanlı olarak yönlendirmeyi önleyecektir.

**Genel Savunmalar: İzinsiz Giriş Tespiti ve Olay Müdahale Prosedürleri**

Bu bölümde açıklanan savunma stratejilerinin her biri, özel araçlar ve saldırılarla ilgilidir. Bu stratejilerin her birini kullanmaya ek olarak, kuruluşların ayrıca bir saldırı tespit edip karşılık verebilecek durumda olmaları gerekir. Bu yetenekler izinsiz giriş tespit sistemlerinin (IDS'ler) kullanılması ve olay müdahale prosedürlerinin uygulanması ile gerçekleştirilir.

IDS'ler ağda hırsız alarmı görevi görür. Bilinen saldırı imza veri tabanına sahip bir IDS, bir saldırının ne zaman yapılacağını belirleyebilir ve güvenlik ile sistem yönetimi personelini uyarabilir. Erken uyarı sistemleri olarak hareket eden IDS'ler, bir kuruluşun erken aşamalarında bir saldırı tespit etmesine ve yol açabilecek hasarı en aza indirmesine izin verir.

Belki de IDS'lerden bile daha önemli olan, belgelenen olay müdahale prosedürleri, etkili bir güvenlik programının en kritik unsurları arasındadır. Ne yazık ki, sektördeki en iyi savunma sistemlerinde bile, motivasyonu yüksek bir saldırgan ağa nüfuz edebilir. Bu olasılığı ele almak için bir kuruluşun, kuruluşun saldırıya nasıl tepki vereceğini açıklayan önceden belirlenmiş prosedürlere sahip olması gerekir. Bu olay müdahale prosedürleri, saldırı sırasında organizasyondaki kişilerin rollerini belirtmelidir. Komuta ve yükseltme prosedürlerinin zinciri önceden yazılmalı. Krizde bu eşyaların yaratılması maliyetli hatalara yol açacaktır.

Gerçekten etkili olay müdahale prosedürleri, sadece bilgi teknolojisine odaklanmamalı, aynı zamanda çok disiplinli olmalıdır. Bunun yerine, Hukuk, İnsan Kaynakları, Medya İlişkileri, Bilgi Teknolojisi ve Güvenlik organizasyonlarının rolleri, sorumlulukları ve iletişim kanalları belgelenmeli ve iletilmelidir. Bu kuruluşların özel üyeleri, bir olay meydana geldiğinde bir olayı ele almak üzere bir araya getirilmek üzere bir Güvenlik Olayı Müdahale Ekibinin (SIRT) çekirdeği olarak tanımlanmalıdır.   
Ek olarak, SIRT, ekip üyelerinin rollerinde etkili olmalarını sağlamak için olay müdahale kabiliyeti konusunda periyodik çalışmalar yapmalıdır.

Ek olarak, Web barındırma, masaüstü yönetimi, e-posta, veri depolama ve diğer hizmetleri kullanarak bilgi teknolojisi altyapısını dış kaynak kullanan çok sayıda kuruluşla, olay yanıt prosedürlerinin bu dış kuruluşlara uzatılması kritik öneme sahip olabilir. Dış kaynak şirketiyle yapılan sözleşme, hizmet sağlayıcının izinsiz giriş tespitinde, olay bildirimi ve olaya müdahaleye katılım konusundaki yükümlülüklerini dikkatlice belirtmelidir. Güvenlik olaylarını ele almak için özel bir servis seviyesi anlaşması ve servis şirketi personelinin bir SIRT'de bir araya getirilmesi için gereken zaman da üzerinde anlaşılmalıdır.

**Sonuçlar**

Bu saldırı araçlarının sayısı ve gücü artmaya devam ederken, sistem yöneticileri ve güvenlik personeli ondan vazgeçmemelidir. Bu bölüm boyunca tartışılan tüm savunma stratejileri, sistemleri yönetmek için eksiksiz ve profesyonel bir iş yapmaktan kaynaklanmaktadır: sistemde neyin çalıştığını bilmek, yamasını sağlamak, uygun bant genişliğinin mevcut olduğundan emin olmak, IDS'leri kullanmak ve bir Güvenlik Olayı Müdahale Ekibi hazırlamak. Her ne kadar bu faaliyetler kolay olmasa ve çok çaba sarf etse de, özen göstererek, bir kuruluş sistemlerini güvende tutabilir ve saldırı şansını en aza indirebilir. İzinsiz giriş tespit sistemleri ve sağlam olay müdahale prosedürleri kullanılarak, üstesinden gelinebilecek çok gelişmiş saldırılar bile, kuruluş üzerindeki etkiyi en aza indirerek keşfedilebilir. Sağlam savunma stratejileriyle etkili bir güvenlik programı oluşturarak, kritik sistemler ve bilgiler korunabilir.