SALDIRI SENARYOLARI

Herkese Merhaba,

Münkün olan bazı saldırı yöntemleri ve bunlara karşı kendinizi nasıl koruyacağınız hakkında kısa açıklamalardan oluşan küçük bir liste oluşturdum. Yazımda, son birkaç yılda tespit ettiğim bu bilgilerin anlaşılmasını sağlamaya çalışacağım. Şunu belirtmek isterim ki yazımda diğer bilgisayarlara saldırı düzenleme düşüncesi yoktur, zaten bu konu hakkında da çok fazla deneyime sahip değilim. Umuyorum ki okuyacağınız bu yazı bilgisayar saldırıları konusunda daha da duyarlı olmanızı sağlayacak.

1 - Hizmet Aksatma (Denial of Service - DoS)

DoS bir veya daha fazla ağ servisini altüst eder veya tıkar, bu yüzden de servisin arkasındaki kişi veya servisin kendisi ağ ile birlikte kullanılamaz hale gelir. DoS esasen sistem kaynaklarını hedef alır. Tehlike altında olan servisler küçük bant genişliğine sahip olan ve/veya ağa herhangi bir tür servis sunan ve güvenli olmayan uygulamalara sahip sistemlerdir. Bu tür tehlikeleri en aza düşürmek için çeşitli yollar vardır, bunlar akıllı bant genişliği yönetimi, ateş duvarları ve devamlı yazılım güncellemeleri olarak sayılabilir. Derin bir bilgiye sahip olmadan da hacker/cracker/ve-diğerleri gibi kişilerin bu çeşit saldırıları deneyebileceğini bilmelisiniz.

DoS aşağıdakiler gibi sınıflandırılabilir:

a) Sel (flooding).

Sunucu bilgisayara anlamsız birçok veri veya istek gönderilir, bu yüzden de sunucu bilgisayar asıl isteklere gerektiği gibi cevap veremez.

b) Smurfing.

IP yayın sisteminin, bir grup sahte kaynak IP adresi kullanılarak (IP-Spoofing) güçlendirilmiş bir sel (flooding) ile kötüye kullanılmasıdır. Bunun anlamı sahte kaynak IP'li ICMP (Internet Denetim İletisi İletişim Kuralı) yankı paketlerinin (pings) yayınlama yoluyla birçok sisteme gönderilmesidir. Bu olayda sahte IP adresleri hedefin IP adresi ile aynıdır. Bunun yayın servislerine gönderilmesiyle, diğer bilgisayarlar ping ile sahte IP'li bilgisayara cevap verirler (Bu hedefin

ta kendisidir) bu da hedefin sistem kaynaklarını kaybetmesini, bant genişliğini tamamen tüketmesini ve hedef bilgisayarın herhangibir servis isteğine kaşı cevapsız kalması sonucunu doğurur.

c) Bant Genişliği Doldurma / Parçalama Saldırısı.

Bu tür saldırılar TCP/IP implementasyonu içerisinde bulunan hataları, servisleri veya sistemlerin tamamını devreden çıkarmak için kullanırlar.

d) SYN/RST Seli (SYN/RST Flooding).

TCP/IP implementasyonu içerisindeki bir zayıflık sayesinde birçok SYN/RST paketi gönderilerek, hedef üzerinde gelen paketler yüzünden bir tampon taşması oluşturulması sağlanır. Bu da hedefin servis isteklerine karşı cevapsız kalmasını sağlar.

e) Özel DoS.

Özel DoS örneğin web sunucularındaki tampon taşması gibi, hedef bilgisayardaki bir servisin bilinen bir zayıflığını kullanır.

2 - Kötü Niyetli Yazılım (Malicious Software)

Kötü niyetli bir yazılım, güvenlik politikası doğru şekilde ayarlanmamışsa, mevcut değilse veya ihmal edilmişse her zaman sisteme girebilir. Örneğin virüs tarayıcıları, onlar virüsleri sistemden uzak tutarlar. Uygulama seviyesinde çalışan ateş duvarları turuva atlarını ve dağıtık solucanları durdurur.

a) Mantıksal Bomba (Logical Bomb).

Çeşitli şartlar altında sistemlere zarar veren programlardır. Ortaya çıkmaları genellikle program hataları veya işletim sistemi hataları ile tetiklenmeleriyle olur. (Örneğin uygulamalar içerisindeki böcekler)

b) Arka kapılar (Backdoors).

Arka kapı bir program/uygulama içerisine yerleştirilmiş, saldırganın sisteme girmesi için bir kapı açan programdır. Açık kaynaklı yazılımlar kullanıcıların kolayca erişebileceği hale geldiğinden beri bir bakıma

kapalı yazılımlara göre daha güvenli olmuşlardır. Derlenmiş programların güvenliğinden emin olmak için bir yol, programın veya kaynak kodunun üzerinde yapılan değişiklikleri haber vermek üzere sayısal olarak imzalanmasıdır.

c) Kurtlar (Worms).

Kurt kendini birçok bilgisayar ağı üzerinden erişim kazanarak bulduğu birçok sisteme yayarak çoğaltan programdır.

d) Virüs

Virüs kendini dosyalara ekleyen ve eklediği yazılım dosyası çalıştırıldığında aktif olup zararlı kodunu calıştıran programdır.

e) Turuva atları (Trojans).

Truva atı sisteme giren ve kendini aktive eden bilgisayar programıdır (kullanıcının veya başka bir uygulamanın aktive etmesine ihtiyaç duymaz).

3 - Zayıflık istismarları (Exploiting Vulnerabilities).

Bir zayıflığı istismar etmek, bilinen bir zaafın hedef sistem üzerinde yetkisiz bir erişim sağlamak veya zarar vermek amacıyla kötüye kullanılmasıdır. İyi yönetilen sistemlerde zaaf oluşturan zayıf noktaları tespit etmek ve acemi kullanıcılardan korumak internet sayesinde kolay olmuştur. Bunun için tek karşı tedbir sisteminizin her zaman güncel olduğundan emin olmanızdır.

Zayıflık istismarları aşağıdaki gibi kategorilere ayrılabilir:

a) Erişim izinleri.

Saldırgan önemli sistem dosyaları üstündeki zayıf bir dosya iznini kullanmayı dener. Bu normalde yazma iznine sahip fakat yazma işlemenine gerek duymayan sistem dosyalarına yazmak ve onları değiştirmek şeklindedir.

b) Kaba kuvvet (Brute Force).

Kaba kuvvetin anlamı birçok yetki kodu, şifre veya kullanıcı-adı/şifre yi sistemli bir şekilde bir servise veya sisteme erişmek için denemektir. Bu prosedür genellikle otomatiktir.

c) Taşmalar (Overflows).

Uzak sistem üzerinde bir tampon taşması ortaya çıkran program kodudur. Aslında birçok acemi programcı tamponları statik olarak giriş verileri için kullanır, bunun anlamı tampon boyutunun sabit olmasıdır. Daha fazla tampona gerek duyan giriş verisi, tahsis edilmiş olan tampon dışındaki bellek alanına da yazar. Programlama diline ve kullanılan dosya tiplerine bağlı olarak, çalışan gerçek kodun bulunduğu aktif belleğin üzerine yazabilirsiniz. (Ahh tanrım !, burasının sizi düşündürdüğünü umarım) Eğer düzenlenmiş kod belleğe yerleştirilmişse hemen aktif olacaktır. (çünkü tampon doludur). Bu noktada C de yazılmış programların, giriş fonksiyonlarının giriş tamponunu, yazılan giriş fonksiyonları ile ayrıştırarak yerel bir katardan okumak için zorladığı yer tehlikededir. Bu tamponlar yığında yerleşmişlerdir ayrıca burası fonksiyonların kaynak adreslerinin yerleştiği yerdir. Bu tür yolları bilen bir saldırgan kolayca programın asıl yapması gerekenleri değiştirebilir. Kötü ayarlanmış bir web sunucu buna örnektir ve bu tür saldırıları kullanan bir saldırgan için büyük bir ödül olabilir. Aynı zamanda CGI script'leri de tehlike oluşturmaktadır.

(*Not: Bu taşma örneği ile gerçekten zor anlar geçirdim. Bu konudaki bilgilerimi oluşturan tüm kaynaklar Almancadır, ayrıca ben bir programcı değilim. Lütfen bu yazıda gözümden kaçan bir hata görürseniz beni bilgilendirin.)*

d) Yarış koşulu (Race Condition).

Bu tür bir saldırı hassas dosyalara ulaşmayı sağlamak üzere, bir program çalışırken oluşan geçici kararsız bir durumu kullanır.

4 – IP Paket Modifikasyonu

IP paket modifikasyonu TCP/IP nin geçmişine dayanan çok uzun bir yoldur. TCP/IP protokoller ailesi kullanılabilirliği güvenlikten daha önde tutacak şekilde tasarlandı. IP yığınları üzerinde yeni atakların oluşturulması çok fazla yetenek gerektirmektedir, bu tür saldırılara az rastlanır fakat bunun yanında da çok tehlikelidirler.

IP paket modifikasyonu aşağıdaki kategorilere ayrılabilir.

a) Port Şaşırtma (Port Spoofing).

İyi bilinen portları (20/53/80 vs.. portları), paket filtreleme kural kümelerini aşmak için kullanmak alışılageldiktir. (Ateş duvarları)

b) Ufak Parçalara Ayırma (Tiny Fragments).

Sadece 8 Byte boyutundaki paketler paket filtreleyen ateş duvarlarındaki protokol-bayrak/port-boyut-görüntülemeyi aldatabilir.

c) Kör IP Şaşırtması (Blind IP Spoofing).

Bir saldırgan, şifre koruması olmayan UDP tabanlı servislere erişim elde etmek için kaynak IP adresini değiştirebilir, ayrıca bu kaynak IP'nin sahip olduğu izinlere bağlıdır.

d) İsim Sunucusu Şaşırtma (Nameserver ID 'Snooping').

Bu tahmin edilebilir tanıtıcı numarası ile birlikte IP aldatmanın kullanıldığı ve isim sunucusunun ön belleğine (DNS cache) sahte verinin gönderildiği yöntemdir. Bu saldırı DNS-Aldatma olarak da bilinir.

e) Sıra Numarası Tahmini (Sequence Number Guessing).

TCP SEQ/ACK numaraları sıra numaraları tahmin edilebilir bilgisayarlara bağlantı sağlamak amacıyla üretilir. Bu yüzden tüm modern IP yığınları kendi sıra numaralarını rasgele üretirler. Tahmin edilebilir sıra numaraları IP yığınları için uzun zaman büyük bir sorun olmuştur.

f) Uzak Oturum Katıştırması (Remote Session Hijacking).

Sahte paketler yardımıyla, aktif TCP/UDP bağlantılarını başka bilgisayarlara yönlendirmek amacıyla kopartılır. Bunun anlamı hedef bilgisayarın hala gerçek sunucuya bağlı olduğunu düşünmesidir, fakat gerçekte saldırgan ile bağlantıdadır.

5 – İçeriden Gelen Saldırılar.

İçeriden gelen saldırılar İnternetin tamamında meydana gelen saldırıların %80'nini oluşturmaktadır. Bu soruna karşı savaşmanın en iyi yolu bilgisayar sistemini nasıl ayarlayacağını bilmek, her zaman güncelliğinden emin olmak ve iyi korumaktır.

İçeriden gelen saldırılar aşağıdakiler gibi sınıflandırılabilir.

a) Arka Kapı Yazılımlar (Backdoor Daemons).

Saldırganın daha sonra sisteme girebileceği bir port (kapı) açacak olan işlemlerin başlatılmasıdır.

b) Kayıt Değiştirme (Log Manipulation).

Neler olduğuna dair izleri gizlemek için kayıt dosyaları değiştirilir veya tamamen silinirler.

c) Paravanlaştırma (Cloaking).

Sistem programlarının sistemin parçalarına yetkisiz erişimi sağlamak üzere turuva atları tarafından değiştirilmesidir.

d) Koklama (Sniffing).

Paket koklayıcıları yerel olarak düz metin şifreler/kullanıcı-adları gibi kritik bilgileri yakalamak amacıyla kurulurlar.

e) Kör Olmayan IP Şaşırtması (Non Blind Spoofing).

Saldırgan veri transferlerini görüntüleyerek, aktif bağlantılara çengel atabilir veya sahte bağlantı oluşturmakta kullanabileceği birçok bilgiyi elde edebilir.

Kaynak : Internet

Versiyon : 1.1.2
Çeviren : Özgür KOCA
E-posta : ozgurkoca@gmail.com
Web : http://tankado.com

Not:*bbs.textzone.net den yardimlari icin Zero, Chagy, Gexguga ve Elico'ya tesekkurlerimi sunarim*