HAZIRLAYAN
BEDRİ SERTKAYA
bedri@bedrisertkaya.com
Sistem Uzmanı
CEH EĞİTMENİ

IDS,IPS,Firewall Atlatma Yöntemleri

IDS NEDİR?

Intrusion Detection System:Tehdit Tespit sistemi bir ağ cihazına gelebilecek yetkisiz girişleri ve atak vektörlerini tespit etmeyi sağlayan sistemlerdir.Tespit ve loglama gerçekleştirir.

IPS NEDİR?

Intrusion Prevention System:Tehdit Önleme Sistemi bir ağ cihazına gelebilecek yetkisiz girişleri ve atak vektörlerini engellemeyi sağlayan sistemlerdir.

IDS/IPS Programları:

Snort

Tehdit Tespit Çeşitleri:

İmza Tanımlama: Sistem kaynaklarını tehdit eden kötüye kullanımları tespit etme biçimidir.
Anomali Tespiti: Kullanıcıların ve bilgisayar bileşenlerinin davranışsal analizini yaparak tespit etme biçimidir.
Protokol Bazlı Anomali Tespiti:TCP/IP protokolü kullanılarak yapılan anomali tespit biçimidir.

IDS Çeşitleri:

Network Based:Ağ temelli ids çeşidi promiscius mod aktif halde saldırı imzalarını tespit edecek şekilde çalışır.

Host Based:Host temelli ids çeşidi ağa bağlı aygıtı gözlemleyerek sadece ilgili ağa ait olayları gözetler.

Log Dosyası Gözlemlemesi:Oluşturulan log(günlük) dosyaları üzerinden ayrıştırma ve analizine yönelik ids çeşididir.

Dosya Bütünlük Kontrolü Yapan:Sistem dosyalarında ve programlarında meydana gelen değişiklikleri tespit ederek buna göre tespit yapan ids çeşididir.Örneğin sistem programlarına sızmış truva atları vb.

Firewall Nedir?

Güvenlik duvarı bir sisteme yetkisiz girişleri engellemeyi sağlayan donanımsal, yazılımsal ya da ikisinin karışımından oluşan sistemdir.Güvenlik duvarı iç ağa gelen ve ağı terk eden bütün mesajları ve paketleri kontrol eder.Yetki ihlali yapanları engeller.

Güvenlik Duvarı Bileşenleri:

Bastion Host:Ağ kaynaklarını yetkisiz girişim ve saldırılara karşı korumayı sağlayan sistemlerdir.

Bu sistemlere "kale", "nöbetçi kale" anlamına gelen tabya (bastion host) denir. Tabyamız, fiziksel olarak iki farklı ağa bağlıdır: iç ağ (Intranet) ve dış ağ (Internet). Tabya iki özelliğe sahiptir:

Yüksek güvenliğe sahip olmalıdır -- yani bu makinaya izinsiz erişim son derece zor hale getirilmelidir.
İki (bazen üç) fiziksel ağ bağlantısına sahip olmalı ve bu farklı ağlar arasındaki iletişimin nasıl yapılacağına dair karar verebilmelidir.

DMZ:(Demilitarized Zone):Arındırılmış bölge ,güvenlik duvarı tarafından daha az korunan, daha fazla erişime izin verilen bir bölgedir. Güvenlik duvarına üçüncü bir ağ çıkışı eklenmesi ve Internet'e servis verecek olan makinaların buraya konulması ile oluşturulur.Buradaki makinalar dikkatli kurulmalı, güvenliğe aykırı protokoller vs. burada yer almamalıdır.

Firewall Çeşitleri:

Packet Filtering Firewall:

Güvenlik duvarından geçen her IP paketine bakılması ve ancak belli şartlara uyarsa geçişine izin verilmesi şeklinde uygulanır.OSI katmanından network katmanında çalışırlar.TCP/IP'de bu IP katmanına denk gelmektedir.
Örneğin:

İç ağınızdan kimsenin Internet'de IRC kullanmasını istemiyorsunuz.
Dışarıdan içeriye hiç kimsenin ssh yapabilmesini istemiyorsunuz.

Bu hedefleri gerçekleştirmek için paket filtreleme yöntemleri kullanacaksınız. Paket filtreleme, güvenlik duvarının her fiziksel bağlantısı üzerinde ayrı ayrı ve yöne bağlı (dışarıya çıkışa izin ver, fakat içeriye girişe izin verme) olarak uygulanabilir.
Paket filtrelemede özellikle yapmanız gereken minimum, dışarıdan gelip de kaynağını içerisi gibi gösteren (IP spoofing - IP aldatmacası) paketleri ve devam etmekte olan bir trafiğin parçası imiş gibi gelen paketleri (IP fragments) filtrelemek ve bunların geçişine izin vermemektir. Çoğu saldırı, bu şekilde başlar.

Circuit Level Gateway Firewall:

Devre seviyesi ağ geçidi güvenlik duvarları OSI katmanlarından sunum katmanında çalışırlar.TCP/IP'de bu TCP katmanına denk gelmektedir.Paketlerin üçlü el sıkışma gerçekleştirmesine göre gözlem yaparlar.

Application Level Firewall:

Uygulama seviyesindeki güvenlik duvarları OSI katmanlarından uygulama katmanında çalışırlar. Uygulama bazlı filtreleme yaparak ftp,telnet vb. veri trafiğine engel olurlar. Vekil sunucu gibi konfigüre edilmişlerdir. Web sitesine yapılan GET ve POST isteklerini filtreleyebilirler.

Stateful Firewall:

Yukarıda açıkladığımız üç güvenlik duvarınında bileşiminden oluşan 3 katmanda da çalışan firewall çeşididir.Network katmanında dinamik filtreleme yapılabilmesini sağlar.

Eskiden filtreleme yöntemleri ağırlıklı olarak statikti yani genel olarak ağınıza ICQ paketlerinin girmesine izin verip vermeme kararı söz konusu idi. 2.4 çekirdeği ve iptables uygulaması ile birlikte dinamik filtreleme Linux üzerinde kullanılabilir hale geldi. Aradaki fark, paketin sırf protokolüne bakarak karar vermek yerine, güvenlik duvarının bir bağlantıyı hangi tarafın başlattığını takip etmesi ve çift yönlü paket geçişlerine buna göre karar vermesidir. Yani bir telnet bağlantısında her iki taraftan da paketler gelir ve gider. Fakat dinamik filtreleme ile, bir telnet bağlantısı iç ağınızdan başlatılmışsa izin verir, başlangıç istemi dış ağdan gelmişse reddedilebilir.

Firewall Tespit Yöntemleri:

Port tarama yöntemiyle hedef sistemde firewall olup olmadığı tespit edilebilmektedir.

Örnek olarak nmap'in firewall eklentisinden faydalanabiliriz.

nmap --script=firewalk --traceroute

Kaynak:http://nmap.org/nsedoc/scripts/firewalk.html

NMAP ile IDS/IPS Atlatma Teknikleri:

Fragment Packets (-f): nmap -f opsiyonu ile TCP paketinin içeriği parçalanır. TCP başlığı üçe bölünerek gerçekleştirilir. (2 8-bit , 4-bit şeklinde). .-f -f (-f iki kez) girildiği takdir de daha verimli olur.Bu şekilde 16-bit paket ve kalan 4 bit paket gönderimi sağlanır.
MTU (–mtu): Değiştirilebilir mtu değeri sayesinde paketler 8'in katları olacak şekilde parçalanabilir.
Kaynak Port Sahteciliği (-g):
Rastgele Paket Ekleme (–data-length): Bu opsiyon sayesinde paket boyutu değiştirilerek firewall atlatılabilir.Default olarak paket boyutları :TCP (40-bits) ya da ICMP (28-bits)
Randomize Hosts (–randomize-hosts): Taranması gereken host aralığını rastgele yapar.
:

Send Bad Checksum (–badsum): Checksum değerinin içine Nmap gereksiz checksum paketleri gönderir.Normal hedef paketi keser fakat ids ve ips rst paketi ile cevap döner.

Set TTL (–ttl): Bu opsiyon nmap'in firewall tespiti yapmasına olanak verir.

Kaynak:http://pentestlab.wordpress.com/2012/04/02/nmap-techniques-for-avoiding-firewalls/

Web Application Firewall Tespiti:

wafw00f programı ile web uygulama firewall tespit edilebilir.

Kullanım:

wafw00f www.hedef.com

HoneyPot Nedir?

Honeypot(Balküpü) saldırganları yanıtlmak amacıyla oluşturulmuş saldırıları ve sisteme sızma girişimlerini kaydeden sistemlerdir.

HoneyPot Programları:

KFSensor, Specter

IDS/IPS Atlatma Teknikleri:

Fragmentation Attack:

MTU(maximum transmission unit) ağa girecek maksimum kapasitedir. Ethernet ağlarında bu değer 1500 byte'dır.Gönderdiğimiz paket ethernet ağındaki router'a geldiğinde 1800 byte ise 1500 olan kısmı parçalanır ve kalan 300 byte ile tekrar birleştirilerek alınır.

Paket parçalalama teknikleri:

fragroute aracıyla ids atlatılabilmektedir.

Fragroute linux işletim sisteminde kullanılabilmektedir.

Gerekli ayarları yapmadan fragroute kullanılamaz.

Fragroute Kullanımı:

apt-get install fragroute komutu ile yüklenir

root yetkisi elde edildikten sonra;

komutu girilir:

echo “0″ > /proc/sys/net/ipv4/conf/all/rp_filter

fragroute programı çalıştırılır:

fragroute -f /etc/fragroute.conf hedefip

ngrep paket yakalama programı çalıştırılır:

ngrep -d any -q -i -q '/etc/passwd'

telnet ile örnek komut girilir:

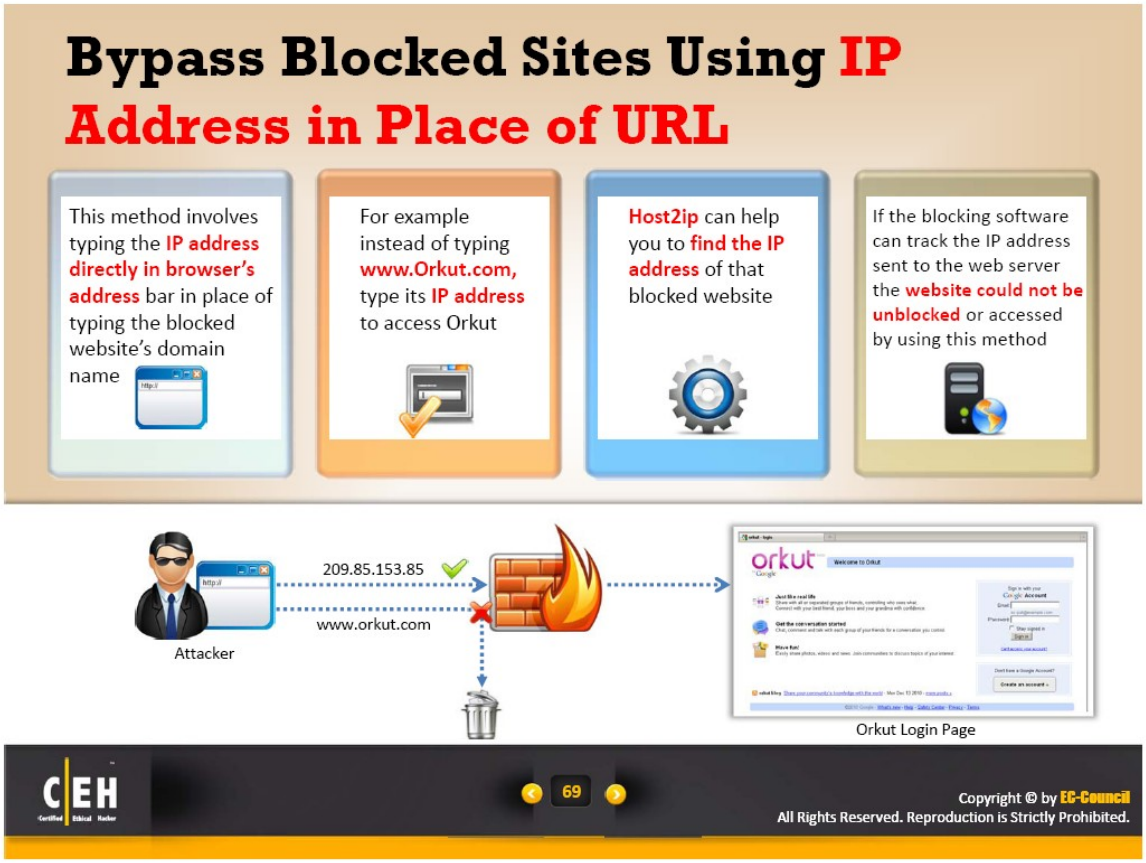
telnet hedefsite.com 80

GET /etc/passwd HTTP/ 1.0

fragroute aktifken yani paket parçalama işlemi olunca ngrep bu isteği yakalayamaz.

rp_filter aktifken ve fragroute pasif olduğunda ise istek ngrep tarafından rahatça yakalanır.

Kaynak:http://www.exploit-db.com/wp-content/themes/exploit/docs/362.pdf



Şekil 1: Engellenmiş web sitelerine ulaşmak için kullanılabilecek yöntemlerden birisi adres yerine web sitesinin ip numarasını kullanmaktır.Yine benzer şekilde engellemesi yapılmış web sitelerine ulaşmak için alt alan adları kullanılabilir.

Örnek:twitter.com kapandığında mobile.twitter.com adresi kullanılarak siteye girmek mümkündü.