

IPS Güvenliđi ve Zafiyetleri

Fatih Özavcı

fatih.ozavci at gamasec.net

Başlıklar

- IPS Mimarisi ve Yerleşimi
- IPS'lerin Kendini Koruması
- Saldırı Tanımlama Zorlukları
- Atlatma Yöntemleri
- 0 Gün Saldırıları

* Host IPS Sunum Konusu Dışında Tutulmaktadır

IPS Mimarisi ve Yerleşimi

- Yerleşim Türleri
 - Ağ Geçidi (Proxy)
 - Köprü Modu (Transparent)
 - Karma (Ağ Geçidi + Köprü)
- Ağ Konumlandırması
 - Kriptolu Trafik
 - DMZ
 - Güvenlik Duvarı
 - Kablosuz Ağ
 - Sanal Özel Ağ
- Saldırı Saptama Türü
 - Olağan/Olağan Dışı Ayrımı
 - İmza Temelli

IPS'lerin Kendini Koruması

- IPS Saptama ve Analizi
- Veri ve Protokol Yorumlama
- İşletim Sistemi ve Platform Zafiyetleri
- Uzaktan Yönetim ve Veri Depolama
- Yayınlanmış Güvenlik Açıkları

IPS Saptama ve Analizi

- Eski ve Çok Bilinen Saldırıların Kullanımı (%c0%af)
- Eski ve Çok Kullanılan Kabuk Kodların Kullanımı (cmd.exe)
- Web Uygulamalarına Özel Saldırıların Kullanımı (SQL Injection, XSS)
- Bilinen Saldırıların Farklı Biçimlerde Kullanımı (Dil Kodlama, Sıkıştırma, Farklı Protokol Kullanımı)
- Eskiden Yeniye Saldırıları Yaparak Güncelleme Sıklığını Belirleme
- Kriptolu İletişimde Tepki Analizi (SSL, TLS, IPSEC)
- Engelleme Türü Analizi (TCP/RST, ICMP Hata Mesajı, Göz Ardı Etme, Süreli Engelleme)
- Basit ve UDP Temelli Saldırı Analizi (Süreli Engelleme ve IP Sahteciliği)
- Sahte Saldırıları ve Hedefleri Kullanarak Gizlenme

Veri ve Protokol Yorumlama

- Ön İşlemcilerin Yeterliliği
 - Parçalanmış Paketler ve Oturumlar
 - TCP/IP Oyunları (TTL, Paket Uzunluğu vb.)
 - Protokol Oyunları
 - Kriptolama ve Kodlama
 - Yoğun Veri Trafiğinde Davranışları (Gigabit)
- Yorumlama Zafiyetleri
 - Hatalı Yorum (Var/Yok)
 - Kötü Programcılık (Bellek Taşması, SQL Inj.)

İşletim Sistemi ve Platform Zafiyetleri

- İşletim Sisteminde Bulunan Güvenlik Açıkları
 - Windows / Linux / AIX / Solaris
- Uygulama Platformunda Bulunan Güvenlik Açıkları
 - SSL (OpenSSL Kütüphanesi Açıkları)
 - Kodlama (Utf-8 vb. Dil Kütüphanesi Açıkları)
 - Sıkıştırma (Gzip/Zip/Rar Kütüphaneleri Açıkları)

Uzaktan Yönetim ve Veri Depolama

- Alternatif Erişim IP'si veya Kanalı Tanımlamaları
- Yönetim Zafiyetleri (RDP, X Server, Özel Yönetim Konsolu, SSL/TLS Servisleri)
- Veritabanının Sürekli Etkin Durumda Olması Gerekliliği ve Kapasitesi
- Saptanan Saldırıdan Kaydedilecek Bilgiler (Paket, Veri, Başlık Bilg. vb.)
- Güncelleme ve Sürüm Yükseltme Zorlukları

Yayınlanmış Güvenlik Açıkları

- Cisco IOS IPS bypass security
<http://xforce.iss.net/xforce/xfdb/22926>
- Cisco Intrusion Prevention Systems CLI gain privileges
<http://xforce.iss.net/xforce/xfdb/21947>
- Block While Proventia Detection Stopped
<http://xforce.iss.net/xforce/xfdb/20786>
- Multiple vendor antivirus/IDS devices bypass detection
<http://xforce.iss.net/xforce/xfdb/18882>
- 3Com TippingPoint IPS page fault detection bypass
<http://xforce.iss.net/xforce/xfdb/27934>
- TippingPoint IPS HTTP traffic denial of service
<http://xforce.iss.net/xforce/xfdb/24200>
- Attack Mitigator IPS 5500 HTTP denial of service
<http://xforce.iss.net/xforce/xfdb/17125>
- McAfee IntruShield allows access any account without authentication
<http://xforce.iss.net/xforce/xfdb/21276>

<http://xforce.iss.net/xforce/search.php?type=2&pattern=ips&x=0&y=0>

Saldırı Tanımlama Zorlukları

- Zafiyet
- Saldırı Türü
- Kabuk Kodu
- Protokol Çözümleme
- İstemcilere Yönelik Saldırıları

Zafiyet / Güvenlik Açığı

- Her Uygulamada Farklılık Gösterir
- Çok Platformlu (x86,sparc,powerpc) ve Çok İşletim Sistemli Uygulamalarda Tek Tanımlama Kullanılamaz (aix, linux, solaris, hp-ux, *bsd, windows)
- Üreticiler, Ürünlerinin Her Açığı ve Açıkların Her Kullanım Yöntemiyle Yayınlamazlar
- Bir Saldırının Bilinen Binlerce Uygulama Yöntemi Olabilir (Encoding, Kripto, Anlamsız/Özel Anlamalı Karakterler, Pipe Kullanımı vb.)
- Ağ Protokolleri, İstemci ve Sunucu Arasında Farklı Yorumlanabilir, Açığın Kullanımını Farklılaştırabilir
- Yönetimsel ve Yapılandırmadan Kaynaklanan Zafiyetler

Saldırı Türü

- Aynı Zafiyet Çok Farklı Yöntemlerle İstismar Edilebilir (FTP, SMTP, HTTP, E-Posta, IM, Resim Dosyası vb.)
- Aynı Zafiyet Farklı Girdilere Farklı Tepkiler Üretebilir (SQL Injection, Buffer Overflow, XSS vb.)
- Saldırı Tanımlanmış Bir Açık Yerine İhmal Edilen Bir Yönetim Arabirimine veya Uygulamaya Yönelebilir
- Saldırı Servis Engelleme Saldırısıdır, Gelen Tepki ile Döngüye Sokulabilir
- Polimorfik Bir Saldırı Sözkonusudur, Açığa Yönelik Her Bir Saldırı Her Seferinde Farklı Olabilir

Kabuk Kodu

- Zafiyet ve Saldırı Türü, Tanımlamada Yeterli Değilse Kabuk Kodu İncelenir
- Polimorfik Kodlama Yapılarak Çözümleme Engellenebilir (Shikata Ga Nai, Alpha2 Unicode, DWORD XOR, Polymorphic Jump/Call XOR)
- İşletim Sistemi ve Sürüm Farklılıklarına Göre Farklı Kabuk Kodları Kullanılır (SP1 vs SP2)
- Kabuk Kodları Açıktan Açığa Farklılık Gösterir (Race Condition, Buffer Overflow, SQL Injection)
- Dil Kodlaması Yapılarak Çözümleme Engellenebilir

Protokol Çözümleme

- Hangi Protokoller (PostgreSQL, MsSQL vb.)
- Hangi Tür Protokoller (Text, Binary, Block, Stream)
- Hangi Protokol Sürümleri (HTTP 1/1.1 vb.)
- Üretici Tarafından Yapılan Uzantılar (WebDAV/Frontpage, SMTP/ESMTP)
- Kriptolu Protokolleri Karşılama (IPSEC, PPTP, SSL/TLS, SSH, SQL+TLS, Netcat+SSL)
- Oturum Durumu Çözümleme
- SMB Protokolündeki Farklılıklar ve Sürümler
- RPC Servisleri (HTTP, UDP, TCP, SMB vb.)
- Web Servisleri (SOAP vb.)

İstemcilere Yönelik Saldırıları

- Web İstemcileri
 - ActiveX, JavaScript, Flash, Sıkıştırma, Dil Kodlama, Bellek Taşması, Spyware
- Acil Haberleşme Yazılımları
 - Msn, Yahoo, iChat AV, Jabber, Kurumsal IM
- E-posta Yazılımları
 - ActiveX, JavaScript, Flash, Sıkıştırma, Dil Kodlama, Bellek Taşmaları, Virus, Worm, Spam, Phishing
- Bu Yazılımların Yayınlanmış Güvenlik Açıkları

Atlatma Yöntemleri

- TCP/IP Oyunları
- Web Uygulamaları
- Kripto Kullanımı
- Sahte Saldırıları

TCP/IP Oyunları

- Yoğun Veri Trafiği Üretimi ve Protokol Çözümlemeyi Devre Dışı Bırakmaya Zorlama
- IP ve TCP Paket Parçalama
- TTL ve Paket Boyu Oyunları
- TCP Seçenekleri ile Oynama (Bayraklar, Sıra Numaraları vb.)
- IP Sahteciliği
- Protokol Özelliklerinin Kullanımı (SMB, RPC vb.)

Web Uygulamaları

- Zafiyetler Yayınlanmış ve Tanımlı Değildirler
- Her Uygulama ve Yorumlama Farklıdır
- Hedef Tanımı Zordur; Uygulama, Yorumlayıcı, Sunucu, Veritabanı vb.
- Encoding Farklılıkları Yorum Hataları Oluşturur
- Oturum Oyunları Takip Edilemez
- Yetki Aşım İhlalleri Kontrol Edilemez
- Normal Kullanım İhlalleri Tanımlanamaz

Kripto Kullanımı

- Kriptolu Protokoller Kullanma (SSL, TLS, IPSEC)
- Kabuk Kodlarını Kriptolama (Polimorfik, Dil Kodu vb.)
- Arka Kapıları Kriptolu Kullanma (nc+ssl)
- Dil Kodlarının Farklı Kullanımı (Utf-8, %u)
- Girdileri Zafiyeti Olan Uygulamanın Açabileceği Biçimde Kriptolu Gönderme (Base64, XOR vb.)

Sahte Saldırıları

- Çok Sayıda Sahte Saldırı ile Gizlenmesi (UDP, DOS, Port Tarama)
- IP ID Oyunları ve IP Sahteciği Kullanımı (Zombi Taraması)
- UDP Temelli Saldırıları ile Farklı Sistemlerin Süreli Engellenmesi
- Sürekli ve Küçük Saldırıları ile IPS Veritabanının Doldurulması (Veritabanı ve Dosya Sistemi Limitleri)
- IP, DNS, ARP Sahteciliği Kullanımı

0 Gün Saldırıları

- Yayınlanmamış Zafiyetler
 - Zafiyet Tanımsızdır ve Öngörülemez
 - Kabuk Kodu Kriptolanabilir
 - Saldırı Türü Normal Süreçlerle Gizlenebilir
- Yayınlanmış Ancak Yamasız Zafiyetler
 - Zafiyet'in Tek Türü Tanımlıdır
 - Uygulama Tepkisi Tam Analiz Edilmemiştir
 - Kabuk Kodu Kriptolanabilir
 - Saldırı Türü Normal Süreçlerle Gizlenebilir

Referanslar

- **Thermoptic Camouflage**

<http://www.metasploit.org/confs/blackhat2006/blackhat2006-thermoptic.pdf>

- **Metasploit Framework**

<http://www.metasploit.org>

- **Polymorphic Buffer Overflow**

http://www-static.cc.gatech.edu/classes/AY2003/cs6265_fall/pallavi.ppt

- **IDS/IPS: Too Many Holes?**

http://www.darkreading.com/document.asp?doc_id=99581