BİLGİSAYAR GÜVENLİĞİ

Hacker & Cracker

Hacker; işletim sistemini tam manasıyla bilen, derinliklerine inen, programlamayı profesyonel düzeyde bilen bilgisayar uzmanlarıdır. Bu dehalar zarar verme girişiminde bulunmaz.

Cracker'lar, genellikle kötü niyetli, menfaat ve geliri için çalışan; sistemlere girme amaçları, veri çalma, zarar verme, işleyişi aksatma gibi olumsuzluklar olan kullanıcılardır.

Lamer, hacker olma özentisi güden, bu amaç için çalışan, programlama bilgisi olmayan kişilerdir.

Bilişim Suçları

-Bilgisayar sistemlerine ve servislerine yetkisiz erişim ve dinleme

-Bilgisayar Sabotajı

-Bilgisayar yoluyla dolandırıcılık ve sahtecilik

-Kanunla korunmuş bir yazılımın izinsiz kullan

Veri Toplama Aşaması

Hedef sistemi tanıdığı zaman yapılacak olan saldırılar şekillenir. Bir korsan için hedefi en iyi tanımanın ilk yolu;

-Whois Veritabanı

-DNS ve IP Veritabanı

-Domain Registration

bilgilerinin elde edilmesidir.

Whois Veritabanı Sorgulama

Korsan sizinle ilgili öğrenmesi gereken ilk bilgileri Whois veritabanından alacaktır.

DNS adresleri, Domain'in bitiş süresi, IP adresi, alan adınızın Name Server bilgileri, Domain'i kaybeden kullanıcının irtibat adresleri, e-mail adresi, telefon bilgileri gibi önemli detayları Whois veritabanında bulunur.

-http://www.allwhois.com

-http://whois.sc

- Saldırgan Whois veritabanındaki bilgileri aldıktan sonra IP veritabanlarını sorgulayarak , sisteminizin subnets(alt ağ blokları) profilini çıkardı. Sonra da DNS sorgulaması yaparak, yapılandırma hatalarını yokladı. Bununla yetinmeyip arama motorlarından siteniz hakkında birçok detaya ulaştı. Hatta kodlama aşamasında hata yapıp yapmadığınızı test ederek, hata yapmışsanız şifrelerinizi bile aldı.

Peki bu profilin çıkarılmasına engel olmak için yapabilecekeriniz neler?

- -Alan adınız kurumsal bir domain değilse -.tr uzantısı ile sonlanmıyorsa- **Private Domain** yani özel domain haline getirmeniz sizi büyük ölçüde tehlikelerden koruyacaktır. Birçok önemli bilginiz Private durumuna geçecektir ve alakasız bilgiler olacaktır.

- Kayıt e-posta adresini sadece domain yönetimi için kullanmanız güvenliğinizi daha da arttıracaktır.

Saldırı Hazırlık Evresi

- Önceki evrede elde ettiği veriler, sisteminizle ilgili sadece yüzeysel verilerdi. Bu evrede ise korsan, ağ ve portlarınızın durumunu ve (PC veya sunucu için) kullandığınız işletim sistemi gibi önemli bilgileri öğrenmek isteyecektir.

İşletim Sistemini Tespit Etme

- Şimdiye dek yazılan her işletim sisteminin, belirli sistem hataları veya sistem açıkları bulunmuştur. Korsan işletim sistemini belirleyerek, her sistemin ayrı ayrı açıklarını denemek yerine kullandığınız işletim sisteminin açıklarını sömürecektir.

- TCP FIN taramaları, ACK paketleri, nmap, p0f, Ettercap, PRADS gibi yazılımlarla işletim sistemi tespit edilebilmektedir.

Korunmak İçin Neler Yapabilirim?

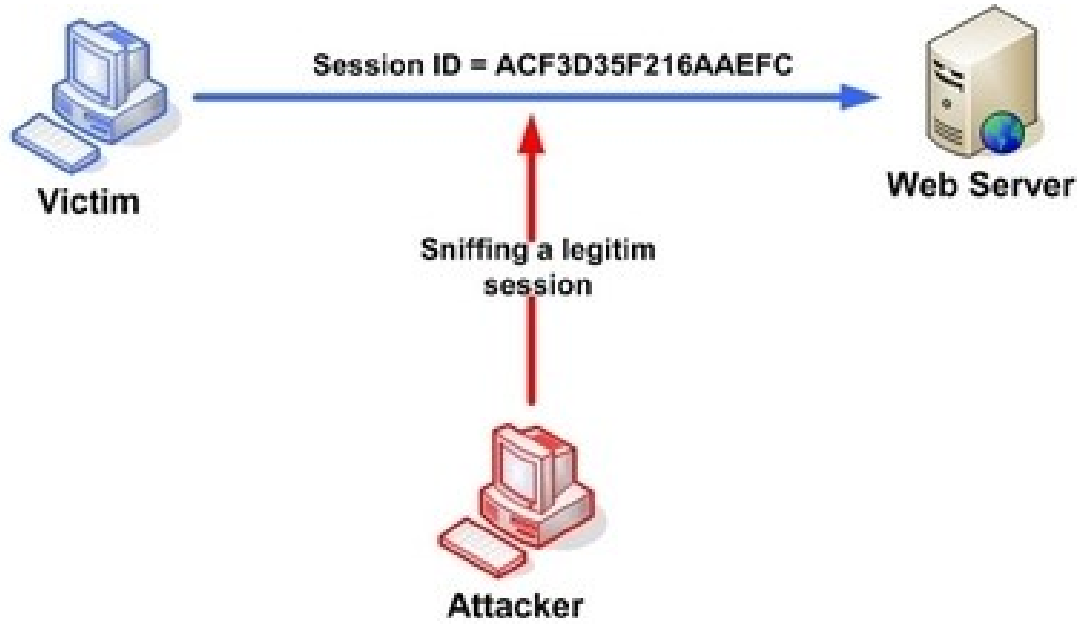
- Teknik olarak yapabilecekleriniz çok sınırlıdır.
- SYN-FIN taramalarını engelleyebilecek kapasitede bir Firewall kullanın.
- Kullanılmayan port ve servisleri kapatın.

Saldırı Aşaması

- Sisteminiz hakkında yeterli bilgi toplayan bir korsanın sıradaki işi, saldırı girişiminde bulunmaktır.
- -Cookie Hi-Jacking
- -ActiveX Saldırıları
- -TELNET(Terminal Network) Saldırıları
- -FSO (File System Object) Uygulaması ve Saldırısı
- -Güvensiz e-postalar
- -Domain Hi-Jacking
- Hizmet Aksatma Saldırıları

Cookie Hi-Jacking

- Terim olarak Cookie; tanımlama bilgileri sunucu bilgisayarlar tarafından işlemci bilgisayarlara yerleştirilen küçük dosyalardır. Bu dosyalar, hazırlamış olduğunuz web sayfasına veya daha önce giriş yaptığınız bir web sitesine tekrar bağlanmak istediğiniz zaman sistem tarafından hatırlanmanızı sağlar. Cookie'ler bu işi, daha önceden bağlandığınız web sunucusuna hatırlatarak yaparlar.



Cookie Hi-Jacking yani tanımlama bilgilerinin çalınması Sniffer yazılımlar, Trojanler veya Cross Site Scripting gibi saldırılarla yapılmaktadır.

Korunma Yöntemleri

- Güvenli HTTPS Protokolü kullanın.
- HTTPS protokolü browser-sunucu arasındaki cookie iletişiminde üçüncü şahısların , tanımlama bilgilerini okuyamayacakları şekilde aktarılmasını sağlayan kurallar içerir.
- Tanımlama bilgilerine sınırlama getirin.
- Standart ayarlarda bilgisayarınız tüm cookie'leri kabul eder, ama bunu istediğiniz gibi değiştirebilirsiniz. Tarayıcıyı her kapattığınızda silinmesini sağlayabilirsiniz.

ActiveX Saldırıları

- ActiveX denetimleri vasıtasıyla Microsoft işletim sistemi , karşı bilgisayarlarda güncellemelerin yüklü olup olmadığını kontrol eder, yüklü değilse yüklenmesini sağlar. Bu uygulamalar vasıtasıyla, sistemin neredeyse tüm bilgilerine erişilebilir.

- İmzalanmamış yani sertifikasız ActiveX uygulamaları güvenli değildir. Sisteminiz hiç tanımadığınız birileri tarafından port açılabilir, çalışan uygulamaların listesi alınabilir, sistem bilgileriniz izlenebilir.

FSO Saldırısı

- FSO(File System Object), çalıştığı sistemin üzerinde bulunan dosya ve klasörleri listeleyen, listelediği dosyalar üzerinde kopyalama, değiştirme, silme, taşıma gibi birçok değişikliği yapan ASP programlama dili tabanlı bir nesnedir.

- Sisteme sızmaya çalışan korsan hem sistem üzerinde dosya, dizin tabanlı birçok değişikliği yapabilecek hem de sistem hakkında bilgi alabilecektir.

Korunma Yöntemleri

- -Güncel IIS kullanın.
- -FSO ile gelen yüklemelere sınır getirebilirsiniz. Mesela .exe, .asp, .php gibi dosyaların yüklenmesini engelleyebilirsiniz.
- -Klasör ve dizin yetkilendirmenizi gözden geçirin.

KOMUT SALDIRILARI

SQL INJECTION

SQL(Structured Query Language), veri tabanlarına erişim ve yönetim için kullanılan standart bir yapıdır. Veri tabanı ile uygulama arasındaki iletişimi sağlar.

Veritabanına SQL ile veriler işlenirken araya bir takım karakterlerin eklenmesiyle de SQL Injection oluşur. SQL Injection ile bir korsan mevcut verilerle oynayabilir, sistem üzerindeki kayıtlara ulaşabilir, yeni kayıt ekleyebilir, silebilir ve değiştirebilir.

SQL INJECTION

SELECT * FROM memberlist WHERE user=‘ ’ OR ‘ ‘= ‘ ‘ AND password=‘ ‘ OR ‘ ‘=‘ ‘

Bu satırdaki hedef kullanıcı bilgileridir.

SELECT Username FROM ExampleTable WHERE UserName=‘ ‘; SHUT DOWN WITH NOWAIT; ‘ AND Password=‘ ‘

Yukarıdaki örnekte ‘; SHUT DOWN WITH NOWAIT diye bir kullanıcı olmadığından dolayı, SQL böyle bir kaydın olmadığına dair mesaj verecektir ancak devamında gelen karakterler SQL sunucusunun kapanmasına neden olacaktır.

KORUNMA YÖNTEMLERİ

- Karakter Filtreleyin

  Filtreleme işlemi tek tırnağı (‘), çift tırnağa ("") dönüştürerek yapılabilir.

- Kayıt Uzunluklarını Sınırlayın

- Kayıt Türlerini Kontrol Edin

  Forma girilen verilerin türlerini kontrol edin.

- Yetkileri Sınırlandırın

  Mümkünse veri tabanına bağlanma işlemi yönetici yetkileriyle değil kısıtlı yetkilerle yapılmalıdır.

EXPLOITLER

Yetkisel kullanıcı profiline yönetsel yetkilerin kazandırılması işlevi Exploiting olarak adlandırılır. Yetki yükseltme işlemlerinin kullanıldığı uygulamalar ise Exploitlerdir. Bir sistemde exploit kullanarak kullanıcı statüsüne yönetici yetkileri verebilmek için, ilgili sistemin sömürülmesi (Exploiting) gerekir.

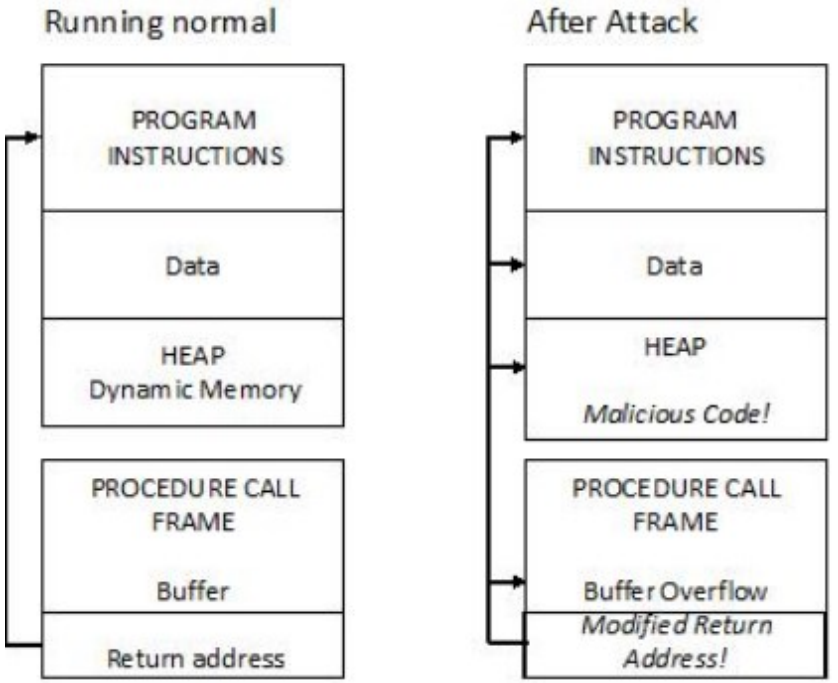
Mevcut işletim sistemlerinin, kullanılan yazılımların ve web uygulamalarının bünyesinde kodlamadan veya başka sebeplerden dolayı meydana gelen açıkların saldırganlar tarafından kullanılması Exploiting işlemi için yeterlidir.

Local Exploitler: Genellikle sisteme (lokal olarak) normal kullanıcı yetkileriyle bağlanan kullanıcıların, yetkilerini yükseltmek amacıyla sistem üzerindeki açıkları sömürmek için kullandıkları exploitlerdir.

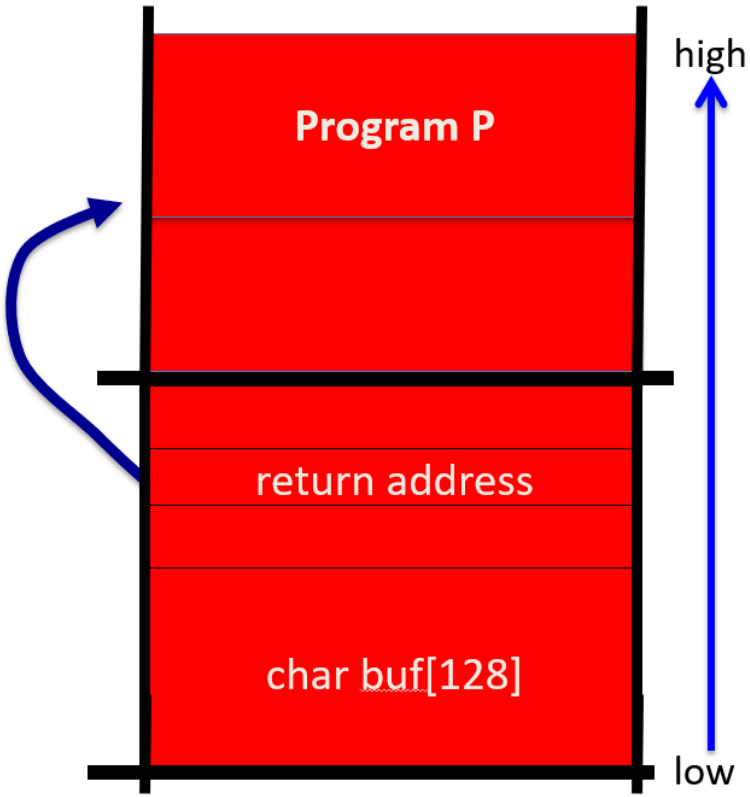
Remote Exploitler: Sisteme (herhangi özel bir yetki olmaksızın) uzaktan bağlanan kullanıcıların uygulamadaki açıkları sömürmek için kullandıkları exploitlerdir.

BUFFER OVERFLOW

Buffer Overflow saldırıları, hafıza alanlarına olması gerektiğinden fazla veri girilmesine dayanır.



Attacker plants code that overflows buffer and corrupts the return address. Instead of returning to the appropriate calling procedure, the modified return address returns control to malicious code, located elsewhere in process memory.



KORUNMA YÖNTEMLERİ

- Dil Seçimi Yapın

  Dil seçimi yaparken doğrudan hafızaya erişime izin vermeyen dilleri kullanmanız faydanıza olacaktır.

- Güvenli Fonksiyonlar Kullanın

  C/C++ birçok tehlikeli fonksiyonu kütüphanelerinde barındırır. Güvenliğiniz için strcpy yerine strncpy, strcat yerine strncat gibi fonksiyonlar kullanabilirsiniz.

- Güvenli Kütüphaneler Kullanın
- Canary Tabanlı Savunma Yapın
- Uygulamanızı Tarayın ve Sisteminizi Güncel Tutun

SOSYAL MÜHENDİSLİK & PHISHING

SOSYAL MÜHENDİSLİK

Sıradan kullanıcı yetkileriyle ilgili sistem hakkında elde edilemeyecek kritik bilgilerin; ikna etme, etkileme, aldatma gibi faktörlerle ele geçirilmesi sosyal mühendislik olarak adlandırılır. Bu yöntemde hedef insanlardır dolayısıyla güvenlik sürecinde savrulması en zor saldırı yöntemi de sayılabilir.

Bir şirketin e-mail, web sistemlerini ele geçirmek veya bazı özel bilgileri elde etmek için bir korsanın yararlanabileceği olası birey potansiyeli şöyledir:

- Yetkili Personel
- Kurum Personeli
- Müşteri Temsilcileri
- Hizmet Alan Kullanıcı

SOSYAL MÜHENDİSLİK

Bir korsan, bireysel olarak internet dünyasında var olan kullanıcının bilgilerini ele geçirmek için şu şekilde davranabilir.

- Hizmet Sağlayıcı
- Teknik Personel
- Yardımsever Kullanıcı

Sosyal Mühendis profilini kullanan bir kullanıcı amacına ulaşabilmek için bazı ikna/etkileme yöntemlerine başvuracaktır:

- Yetkili Görünüm
- Yardımsever Görünüm
- Zaaflardan Faydalanma
- Minnet Altında Bırakma

PHISHING

Phishing, yani oltalama, Internet kullanıcılarının kredi kartı ve banka hesap numaraları, bu hesaplara ait şifre ve CVV2 numaraları gibi bilgileri elde etme amacıyla saldırgan tarafından yapılan sosyal mühendislik saldırısı da denebilir. Bu saldırılarda kandırılan kullanıcı, oltaya takılan balığa benzediğinden dolayı oltalama adını almıştır.

Phishing saldırılarında kullanıcı genellikle sahte e-postalar vasıtasıyla tuzağa düşürülür. Saldırıyı yapan kullanıcı doğrudan temas yerine bilinen ve güvenilen banka ve firmaları kullanarak hedef bilgileri ele geçirmeyi hedefler.

ÖRNEK BİR PHISHING SALDIRISI

From: Garanti Bankasi [mailto:alarmi@garanti.com.tr]
Sent: Wednesday, August 26, 2009 3:26 PM
Subject: Guvenlik Alarmi
Importance: High

Garanti

Guvenlik Alarmi

Turkiye Garanti Online Bankacilik hesabinizin hizmet suresi dolmak uzeredir.
Asagidaki linki kullanarak hesabiniza ulasabilir ve hesabinizi tekrar aktif hale getirebilirsiniz.

https://sube.garanti.com.tr/isube/login/

KORUNMA YÖNTEMLERİ

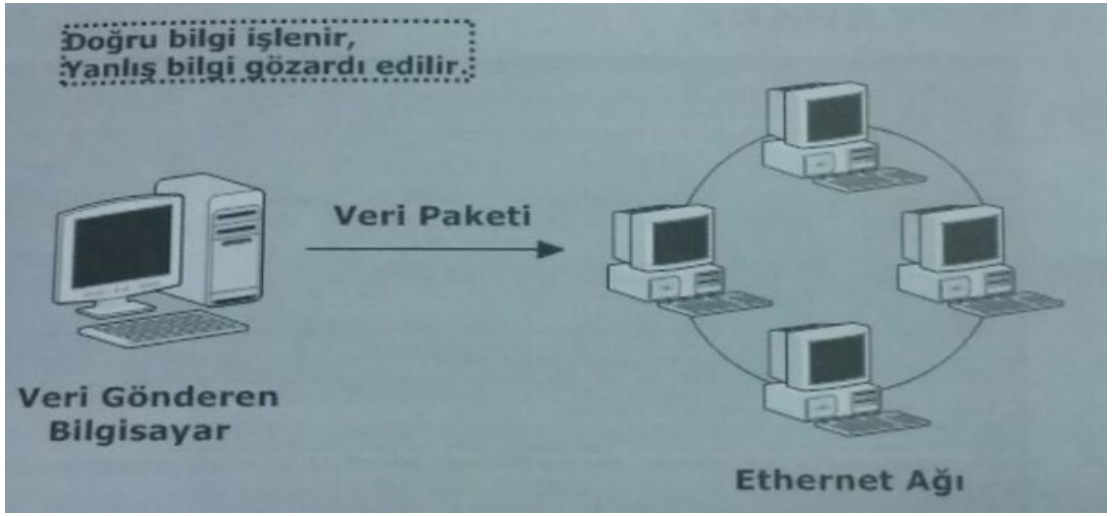
- Güvenilir Kaynak Bilgi İstemez
- Tanımadığınız Mailleri Okumayın
- Adres Kontrolü Yapın
- Güvenli Protokol Kontrolü Yapın
- Hesap Özetinizi Kontrol Edin

İZLEME VE GİZLENME

SNIFFING

Hedef sisteme teknik yöntemler veya Sosyal Mühendislik ile sızmayı başaran bir korsanın yapacağı ilk iş bulunduğu sistemi izleme ve bunu yaparken de gizlenme olacaktır.

Sisteme sızan biri, veri trafiğini, sistem bilgisini ve kullanıcı hesap bilgilerini sistemi **izleyerek** (Sniffing) ele geçirebilir. İşletim sistemi kayıt tuttuğundan dolayı, bu kayıtlara yakalanmamak için de kendini **gizler** (Spoofing).



SİSTEMİ SAHİPLENME

BACKDOOR

Sisteme sızmayı başaran bir korsan, yerini garantilemek, sonradan tekrar bağlanabilmek için Backdoor kullanır. Kullanılan Backdoor araçları sistem yöneticisinden habersiz, korsanın sisteme bıraktığı scriptleri çalıştırabilir ve internet üzerinden sistem ile ilgili detayları korsana iletebilir.

KORUNMA YÖNTEMLERİ

- Sistem/Uygulama Güvenliğini Sağlayın
- Firewall Kullanın
- Backdoor Tespit Araçları Kullanın
- Dikkatli Olun

TROJAN

Trojanlar doğrudan bilinen bir kaynaktan geliyormuş gibi görünerek çalıştığı sistemi ele geçirebileceği gibi kullanıcılar tarafından bilinen ve çeşitli amaçlarla kullanılan yazılımların tahribata uğratılmasıyla da kullanılabilirler. Herhangi bir yazılımın vektör olarak kullanılmadığı Trojan saldırılarında; zararlı dosya resim, oyun, program veya kalıp dosya şekillerinde gösterilir. Böylece kullanıcı tarafından Trojanın çalıştırılması hedeflenir.

Standart bir trojan, bulaştığı sistemde kendi kendini çalıştırabilme yetkisine sahip değildir, mekanizması bu şekilde işlemez. Trojanın bulaştığı sistemde etkili olabilmesi için kullanıcı tarafından çalıştırılması gerekir.

KAYNAKÇA

KODLAB Hacker Interface Kitabı

DİNLEDİĞİNİZ İÇİN TEŞEKKÜR EDERİZ...

MERVE KAYGISIZ

ELİF CANSU YILDIZ