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

BİLGİ GÜVENLİĞİNE GİRİŞ

John Draper’a göre hacking:
Bütün bu tanımlar içinde bana en doğru geleni şu, hacking "programı değiştirmek"tir.
John Draper'ın söyleşisini okumak için:
http://dosyalar.hurriyet.com.tr/hacker/draper.asp

1.Bilgi Güvenliğinin Elemanları

Güvenlik tanımı: Güvenlik bir bilgi ve altyapı evresidir bu durumda başarılı ancak algılanamayan bir hizmet veya bilginin bozulma olasılığını düşük veya tolere edilebilir durumda tutmaktır.

Bilgi güvenliğinin prensiplerini üç temel öğe oluşturur:

Gizlilik:Bilginin güvenli ve açığa çıkmayacak şekilde sadece yetkili olan kişiye sahibine gönderilmesidir.Doğru kişiye gönderilen bilgi vb...

Bütünlük:Bilginin gönderen tarafından bozulmadan ve orjinalliğini yitirmeden iletilebilmesi, alıcı tarafından da alınabilmesidir.

Kaynak:http://it.med.miami.edu/x904.xml

Kullanılabilirlik:Sistemin çalışmasını stabil olarak devam ettirmesidir.İstenilen bilginin istenildiği anda elde edilebilitesidir.

Örnek:Hizmet vermesi gereken bir sitenin hizmet veremeyecek şekilde aksaması.

Hacking:
Savunanlar ve saldıranlar arasında geçen teknoloji geliştikçe sonu gelmeyecek olan bir mücadele.

2.Hacking Terminolojisi:

Hacklenmek istenen hedefin hacker’a kazandıracağı şey ne olabilir?

WHO ARE HACKERS? WHO ARE THEY?

NEWBİES:

Yeni yetmeler genelde bu işe meraklı olurlar. Öğrenmeye meraklı ve heveslidirler. Hayatlarında ilk kez hacking dünyasına girdikleri için öğrendiklerini uygulamada pratik olurlar. Hack teamler ise yeni yetme hackerları bir araya getirerek rütbelendirme sistemi içerisinde bilgi seviyesi ve tecrübesi arttıkça üst kademeye yükseltirler.

Tatmin, ün, zarar vermekten duyulan haz, farkında olunamayan ama faaliyete dönüştürüldüğünde hacker tarafından başarı olarak algılanan hedef çaresiz duruma düştüğünde ve tamamen ele geçirildiğinde ise vandalizme kadar varan hareketler.

Hacker Gruplandırmaları:

Siyah şapkalı hackerlar:Siyah şapkalı hackerlar iyi niyetli olmayan bilgi ve tecrübe olarak ileri seviyede becerileri olan yıkıcı faaliyetlerde bulunan en tehlikeli hacker çeşididir.Temel olarak bir bilgi elde etmeyi ya da silmeyi amaçlarlar. Bilgi silenlerine crackers da denir.
Beyaz Şapkalı Hackerlar:Hacking bilgisini yıkıcı faaliyetlerde değil çalıştığı kurum için yapıcı faaliyetlerde kullanan hackerlara denir. Güvenlik analistleri beyaz şapkalı hacker olarak adlandırılabilir. Sorumlu olduğu sistemdeki zayıflıkları karşı analiz ederek, açıklıkları tespit ettikten sonra,tespit edilen açıklığa karşı nasıl korunabileceğine dair çözüm oluşturur.
Gri Şapkalı Hackerlar:Beyaz şapkalı hackerların yaptıkları işin dışında ofansif olarak da testler gerçekleştiren hackerlardır. Yani iyi işlerin dışında siyah şapkalılar gibi davranabilirler.

Güvenliğe Yön veren Gelişmeler:

Devletin çıkardığı yasalara ve kurallara karşı yapılan eleştiriler.
Teknoloji geliştikçe hackerlar da gelişiyor daha karmaşık ve tespiti zor virüsler ortaya çıkıyor.
Bilgi kaçırma, iç çalışan tehditi,

Güvenlik risklerinin sınıflandırması:

Bilgi ifşası, veri kaybı riski, itibar kaybı
Hedef amaçlı karmaşık saldırılar
Organize siber suç(Anonymous redhack)
Oltalama, sosyal mühendislik saldırıları
Siber Casusluk Faaliyetleri
0 Day Exploits
Vishing yani sahte bankacılık zararlı yazılım saldırılar(En yakın örnek Fatmal,Turkcell)
****
Underground Black Market
Siber Şantaj(Yakın örnek server yedekleri türkiye saldırıları, cryptolocker)
Taşınabilir disklerle gelen tehditler
Botnetler
Yeni gelişen ve talep fazlası teknolojilerdeki 0 days
Cloud teknolojiler

Effects of Hacking:

Sistemleri ele geçirmek için rootkit,truva atları ve gelişmiş virüsler,Zombiler, spam botlar, Verilere zarar verme verileri çalma,Sosyal güvenlik numaraları, kredi kartı numaraları, kişisel bilgilerin çalınma riski,

Kurumsal olarak Hacking'in Etkileri:

Şirketlerin müşteri bilgilerini çaldırması itibar kaybına sebep olur.
Verilerin çalındıktan sonra korsan olarak piyasaya sürülmesi şirketlerin kaybını arttırır.
Botnetler(istismar edilerek ele geçirilmiş zombilerden oluşan bilgisayarlar) erişim engelleme saldırılarında kullanılarak sistemleri işleyemez hale getirebilir ve veri kayıplarına sebep olabilirler.
Saldırganlar önemli belgelerini ve bilgilerini çaldıkları firmaların verilerini rakip firmalarla paylaşabilirler.

- Tehdit – Güvenliğe riske sokacak bütün şeyler.
- Örnek:İnsan da güvenliğe riske sokabilecek en kolay elemandır.
-
- Açıklık – Sistemin ele geçirilmesini sağlayacak bir zayıf nokta.
- Örnek:Zayıf kilitli bir kapı.
- Target of Evaluation – Hacklenmesi gereken hedefin değerlendirilme süreci.
- Güncel Örnek:Adobe gibi büyük şirketlerin hacklenmesi.
- Saldırı – Hedefi ele geçirmek için yapılan girişim.
- Exploit :Açıklığı istismar etmek için kullanılan araç ve bunların tümü.
- 0 Day:Sıfırıncı gün açıklıklar bir uygulamayı veya sistemi etkileyen üretici ve kullanıcılar tarafından henüz tespit edilmemiş siber silahlardır.

Authencity:Özgünlük
Örnek:Veriyi alan ve gönderenin belli olması.
Örnek:SSL

Non Repudiation:Reddememe
Örnek:PGP

Hacking Aşamaları:

Araştırma ve bilgi toplama, tarama ağ keşif tespit,Erişim elde etme,erişimi muhafaza etme,izleri silme

İKİNCİ HAFTA PLANI:

Foot Printing Metodolojisi:

Pasif Bilgi Toplama:

Kendi bilgisayarımızdan değil internet üzerindeki bilgi toplama sitelerinden sorgulamalar

gerçekleştirmek suretiyle bilgi toplayabiliriz.

Bilgi Toplama Süreci:

Hedefle ilgili temel zayıflıkları bulabilmek amacıyla bazı bilgiler toplanır.
Hedefle ilgili Whois Alanadı sorgulama,dns kayıtları vb. Şekilde bilgiler çıkarılır.
Hedef sistemin çalıştığı işletim sistemi ve elemanları tespit edilir.
İstismar edilebilecek olası zayıflıklar tespit edilir.

İz Sürme Sürecinin Hedefleri:

Ağ Keşif Süreci:

Alanadı
İç Ağ Bilgisi
Network Blocks
İnternete açık ip adresleri
TCP ve UDP Portlarında çalışan servisler

Sistem Keşif Süreci:

Kullanıcılar ve Gruplar
Sistem Banner Bilgisi
Routing Tabloları
SNMP Bilgisi

Kurum Bilgisi Toplama:

Çalışanların eposta adresleri
Kurum Websitesi
Kurum tarihçesi
Kurum bağlantıları iş yaptığı yerler

İnternet Üzerinden Bilgi Toplama:

Google,Bing,Pipl

Hedef web sitesi ile ilgili link haritası çıkarma işi:

Link extractor tools
netcraft.com(Hedef sistemin çeşidi,uptime bilgisi)

Hedef şirket ile ilgili bilgi toplama:

Bing ve google'da hedefle ilgili spesifik aramalar yapmanın yanısıra işimizi kolaylaştıran ve bilgi

toplama sürecini kısaltan araçlarda vardır.

1.WebDataExtractor.com websitesi
2.Spider Foot Program
3.Robtex websitesi

Arama motorlarını kullanmak sadece normal arama yapmak demek değildir.Arama motorlarının önbellek özelliği ile silinse bile web sitesi arama motoru tarafından kaydedilmişse geçmişteki bilgiler görülebilir.