BİLGİ TOPLAMA AŞAMASI

Hedef sistemi hakkında bilgi toplama aşaması 2 kısımda oluşur.

Pasif Bilgi Toplama

Pasif bilgi toplamada hedef sistemle ilgili tüm bilgiler internet üzerinden herhangi bir iz bırakmadan, hedefe ait sistem ve sunuculara erişmeden toplanmaya çalışılır. Yani karda yürüyüp iz bırakmama.

Pasif bilgi toplama yöntemleri

1) Whois,
2) DNS sorgularını yapabileceğimiz ve pasif bilgi toplamak için kullanılan özel Web sayfaları (netcraft, robtex, centralops)
3) Arama motorları (Google => deneme filetype:pdf,

   kalem site:google.com

   intitle:index.of passwd

   mail:@ornek.com.tr)
4) Sosyal medya (pipl)
5) Github,
6) Arşiv siteleri(web.archive),
7) Kariyer siteleri,
8) Bloglar ve formlar

Aktif Bilgi Toplama

Pasif toplamada hedefin ip adres bilgilerini ve servis bilgilerini öğrenmiş olduk. Aktif bilgi toplamada ise bu öğrendiğimiz bilgileri kullanarak sistemi taramaya başlayacağız. Temel amaç sisteme sızmanın yollarını aramaktır.

Nmap, ağ güvenlikçilerinin, sistem uzmanlarının ve hackerlerin en çok kullandığı yazılımlardandır.

Temel seviyede yapabildikleri:

İleri seviyede yapabildikleri:

Nessus, ağlarda güvenlik testi yapan ücretsiz bir yazılımdır. Temel amacı bilgisayar sistemlerinde ve ağlarda bulunan zafiyetleri ya da zafiyet oluşturabilecek servisleri ve bilgileri raporlamaktır. Nmap gibi sadece port taraması yapmakla kalmaz, sistem de bulabildikleri bütün açıkları sunar.

KAYNAKÇA

Bilgeiş “Sızma Testine Giriş” eğitimi.