1- BİLGİ TOPLAMA NEDİR VE NEDEN YAPILIR?

Bilgi toplama hedefi tanımaktır. Karşımızdaki hedef ile ilgili ne kadar fazla bilgi edinirsek, hedefi ne kadar iyi tanırsak hedefe ulaşmamız da o kadar kolay olacaktır. Ayrıca işimize yarayacak sağlam bir bilgi toplama ile henüz atağa başlamadan sağlam bir temel oluşturmuş oluruz, yapacağımız atak ile ilgili senaryo hazırlığı yaparız. Böylece daha başarılı ataklar yapabiliriz.

2- BİLGİ TOPLAMA TÜRLERİ

- Pasif Bilgi Toplama
- Aktif Bilgi Toplama

A- PASİF BİLGİ TOPLAMA

Pasif bilgi toplama, hedef ile direkt olarak temasa geçmeden yapılan bilgi toplama işine denir. Sızma testlerinde bilgi toplama işleminin ilk aşamasıdır. Bu aşamada amaç hedefe ait bilgilere, hedefe ait sistem ve sunuculara erişmeden, internet üzerinden bilgi toplamaya çalışmaktır.

OSINT(Open Source Intelligence): Erişimi herkese açık olan kaynaklar üzerinden hedef hakkında bilgi toplamaktır. Sosyal medya hesaplarından yapılan yer bildirimleri, adres paylaşımları, genele açık fotoğraflar, yazılar hepsi birer Osint unsuru olabilir.

Günümüzde birçok pasif bilgi toplama aracı mevcuttur. Çok sık kullanılanlarından bazıları ise şunlardır:

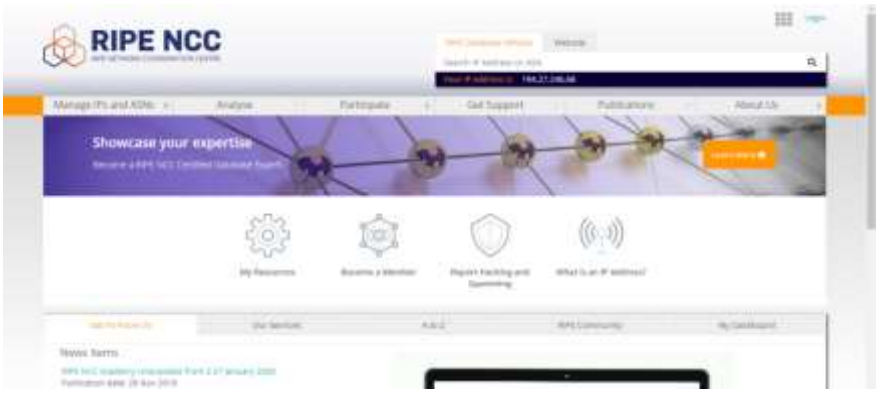
1- Whois: Hedef domain için, name server, admin iletişim bilgileri, tescil ettiren kuruluş veya kişi gibi bilgilerin pasif bilgi toplama tekniği ile elde edilmesinde yardımcı olmaktadır. Yapılan whois sorguları ile aşağıdaki bilgilere sahip olunabilir:

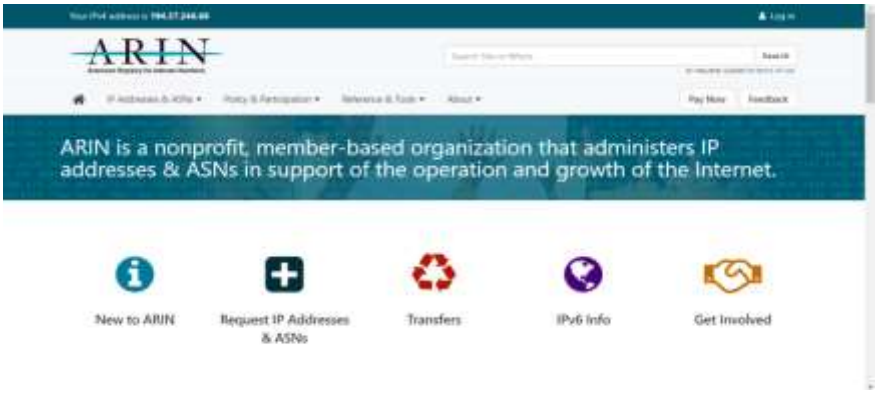
- Kurumun ait olan ip aralıkları tespit edilebilir.
- DNS sorguları ile kurumda çalışan WEB, FTP, MAIL gibi servislerin ip adresleri tespit edilebilir.
- Kayıtlı alan adı(domain) isimlerinin hangi sunucuda tutulduğunu, kontak kişinin bilgisi, mail adresi ve telefon, adres bilgilerine erişilebilir.
- Kurum web sayfasının nerede tutulduğu bilgisi tespit edilebilir.
- Alan Adı(Domain) geçmişi ve bitiş süreleri tespit edilebilir.
- Belirlenen IP adresi üzerinde çalışan diğer web sayfaları tespit edilebilir.

Whois ve DNS sorguları ile bilgi toplamak için aşağıdaki sayfalar kullanılabilir:

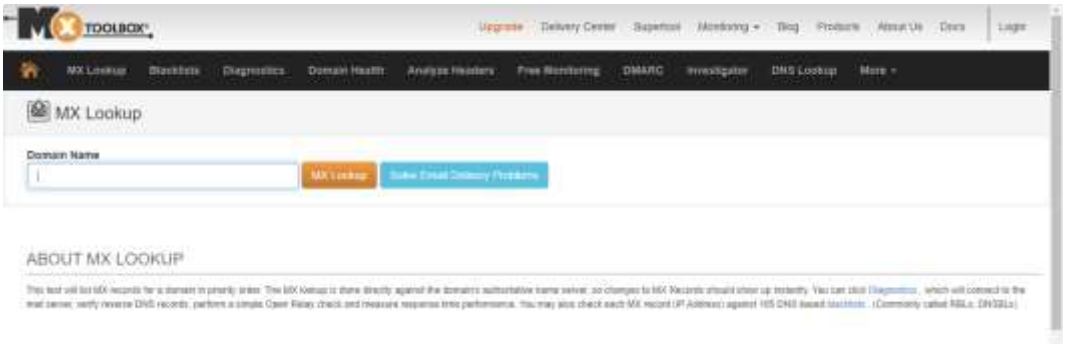
robtex.com: Bu siteyi kullanarak detaylı whois bilgisi ve DNS kayıtlarına ulaşılabilmektedir. Herhangi bir ip adresi için ulaşılabilir web sayfalarının listesini sunmaktadır.

rip.net ve arin.net: Gerçek ip adreslerini dağıtan iki kurum olan Ripe ve Arin üzerinde Whois bilgilerine erişilebilir.





mxtoolbox.com: Bir alan adına ait olan, MX kayıtlarını sorgulamanın yanı sıra bu alan adı ile ilgili olan SMTP Relay, ters DNS sorguları gibi SMTP bilgilerinin toplanması için kullanılmaktadır. Buradan aynı zamanda Whois bilgileri sorgulanabilmektedir.



centralops.net: Site üzerinde bir alan adına ait ip, detaylı Whois bilgisi, dns kayıtları (A,MX,PTR vs) ve TcpQuery bölümünde web sunucu platformuna ait bilgiler elde edilebilir.

archive.org: Bilinen kaliteli arşiv sayfalarından birisidir, birçok sitenin geçmiş versiyonlarını içerisinde barındırmaktadır. Örnek vermek gerekirse www.hotmail.com ‘un **1996** yılındaki sayfasına kadar görebilirsiniz. Geriye dönük bilgi toplamak için kullanılması gereken sayfalardan biridir.

pipl.com: Kişisel bilgi toplama amacıyla kullanılır.

Sosyal paylaşım ağları: Twitter, Facebook, Linkedin gibi sosyal platformları kullanarak kişiler veya kurumlar ile ilgili derin bilgiler elde edilebilmekte ve bunların diğer platform, insan ve kurumlarla olan ilişkileri açığa çıkabilmektedir. Bu detaylı inceleme, aktif bilgi toplama ve daha sonrasında hedefe sızma aşamasında işlemi hızlandıracak hayati bilgilerin ortaya çıkmasına yardımcı olmaktadır.

Arama motorları: Google, Bing, Yahoo ve bunun gibi arama motorlarını kullanarak web sitesi ile ilgili keşfetmek istenilen bilgiler Google’a özel parametreler ile bulunabilmektedir. ‘Google Hacking’ parametreleri bu konuda üstün yarar sağlamaktadır.

DORK: Arama motorları internet üzerinde erişebildikleri tüm siteleri tarayıp, siteleri kaydederler. Arama motorlarının aramalarımızı daha kesin ve kaliteli yapabilmemiz için bize bazı anahtar kelimeler sunarlar. Bu anahtar kelimelere dork denir.

B- AKTİF BİLGİ TOPLAMA

Hedef ile doğrudan iletişime geçilerek yapılan bilgi toplama işlemidir. Sızma testlerinde bilgi toplama işleminin ikinci aşamasını oluşturmaktır. Aktif bilgi toplamada amaç; IP ve servisler üzerinden özel araçlar ve yöntemler ile tarama gerçekleştirmektir. Bilgi toplama esnasında hedef sistemler ile temas sağlanır ve bu temas hedef teki güvenlik cihazlarının log kayıtlarında bulunabilir.

NMAP: Aktif bilgi toplama aşamasında en çok fayda sağlayan ve kullanılan araç NMAP'tir. Taranmak istenen hedef ağın haritasının çıkarılmasında, ağdaki cihazlarda çalışan servis bilgilerinin veya işletim sistemlerinin öğrenilmesinde kullanılan bir güvenlik tarayıcısıdır. Burada hedef sistemde açık olan portlar, buradaki fiziksel aygıt tipleri, cihazların çalışma süresi, hangi servislerin kullanıldığı, kullanılan yazılımların sürüm detayları, güvenlik duvarı bilgileri ve ağ kartına ait diğer bilgiler açığa çıkabilmektedir. Aynı zamanda gelişmiş özellikleri de kullanılmak istenirse zaafiyet keşfi yapılabilmekte ve Güvenlik Duvarı/IDS atlatma girişimlerinde başarılı sonuç alınabilmektedir.

MASSCAN: Masscan NMAP ile aynı sonuçları verebilirken bunu daha hızlı bir şekilde yapmaktadır. Tüm interneti 6 dakikada, saniyede 10 milyon paket göndererek yaptığı iddia edilmektedir.

NSLOOKUP ve DIG: NSLOOKUP Windows sistemlerde bilgi toplanmasına olanak sağlar iken; DIG, Linux ortamlarında hedef kaynak hakkında bilgi sağlamaktadır. DIG, Linux sistemlerin farkından dolayı NSLOOKUP 'dan daha gelişmiş özelliklere sahiptir.

DNS Zone Transferi: DNS sunucusunda alan adının çözülmesi ile ilgilidir. A, MX, NS VE PTR gibi mevcut olan DNS kayıtlarının, birincil DNS sunucu üzerinden bir diğer DNS sunucusuna aktarılmasına ZONE TRANSFER denilmektedir. Bu transfer için izin verilmesi gerekmektedir, verilmiş olan bu izin açıklık yaratabileceğinden bu kayıtlar ele geçirilebilir bilgiye dönüşebilir. Hedefin Host adları ile bunların zaafiyetlerinin bulunması durumunda çeşitli bilgiler ele geçirilebilmektedir.

BANNER ele geçirme: Hedef sistemin kullandığı sistem ve bunun versiyon bilgisine veya varsa diğer açık bilgilere Banner sorgusu yaparak ulaşılmaktadır. NETCAT gibi araçlarla bu sorgu yapılabilmektedir.

MALTEGO: Maltego ile domain adlarının WHOIS, DNS, Ağ yapısı bilgisi ve kişiler ile ilgili bilgi edinilebilmektedir.

Sandmap: Çok sık tercih edilen nmap toolunu kullanarak ağ ve sistemleri keşfetmek için kullanılan bir araçtır. Nmap'e göre kullanıcı arayüzü sağlayarak daha kolay bir deneyim sunar. Nmap Scripting Engine (NSE) desteği ile kullanabildiği gibi, TOR desteği de mevcuttur.

Yasuo: Ruby dili geliştirilmiş third part yazılımları tarayan ve üzerlerindeki açıkları yakalamaya çalışan uygulamadır.

Devploit v3.6: Python ile geliştirilmiş bilgi toplama araçlarından biridir. HTTP başlıklarına, port, GeoIP, Subnet bilgilerine bakmak için kullanılabilir.

Dmitry: Subdomain, email adresleri, açık port taraması, whois sorgusu gibi çeşitli bilgileri elde etmek için kullanılır.