**AKTİF VE PASİF BİLGİ TOPLAMA**

Bilgi toplamak hedefi tanımak için gerçekleştirdiğimiz bir işlemdir. Hedef hakkında olabildiğince bilgi edinerek hedefe ulaşmayı amaçlarız. Topladığımız bilgiler ne kadar detaylı ve doğru olursa hedefe ulaşmamız ve başarılı bir sonuç elde etmemiz o kadar kolay olur.

**Pasif Bilgi Toplama**

Bilgi toplama aşamasında, öncelikle pasif bilgi toplama gerçekleştirilir. Pasif bilgi toplama hedef ile direkt olarak temasa geçilmeden gerçekleştirilen bilgi toplama çeşididir. Bu süreçte kamuya açık kaynakları kullanarak bilgi toplarız ve herhangi bir iz bırakılmaz. Bilgi güvenilirliği düşüktür.

**Google Hacking:**

Google’da bazı operatörler kullanarak istediğimiz bilgiye daha kolay ve hızlı bir şekilde ulaşabiliriz.

site : Arama sonuçlarını domain ile sınırlar. (Örnek:. site:google.com, site:tr)

filetype: İstediğiniz dosya tipini içeren sayfaları görmenizi sağlar. (Örnek:. filetype:pdf)

inurl: Sayfanın url adresinde belirtiğiniz ifade içerenleri gösterir. (Örnek:. inurl:admin.php)

intitle: Sayfanın başlığında belirttiğiniz ifadeyi içerenleri getirir. (Örnek:. intitle:index.of , intitle:”google”)

* : Aramalarımızda başına geldiği kelimeyi aramaya dahil etmez.

+ : Başına geldiği kelimeyi aramaya dahil eder.

**Whois:**

Whois yardımıyla bir internet kullanıcısı herhangi bir domain adresinin ne zaman kayıt edildiği, kayıt süresinin ne zaman son bulacağı yada domain’in hangi firma altında kayıtta olduğu gibi bilgilere ulaşabilir.

**Shodan:**

İnternete açık olan cihazları tespit etmek amacıyla kullanılan bir arama motorudur. Korunmasız herhangi bir cihaz bulunarak varsayılan giriş bilgileri kullanılıp hassas bilgiler elde edilebilir.

**Censys:**

İnternetteki aygıtları tarayarak kaynakların nasıl yapılandırıldığı ve dağıtıldığı hakkında toplu raporlar verir. Her kamusal IP adresini ve popüler domain’leri düzenli olarak tarar.

**Netcraft:**

Sorgulanan IP adresi veya domain’in işletim sistemi, web sunucusu çalışma süresi(uptime) hakkında bilgiler edinebileceğimiz sitedir. Ayrıca web sitelerinin daha önce kullandığı IP adresi, işletim sistemi, server bilgilerine de ulaşabiliriz.

**Wayback Machine(Archive.org):**

Sitelerin eski hallerini görmemizi sağlayan bir [web](https://wmaraci.com/nedir/web) sitesidir. Web sitelerini belirli aralıklarla tarayarak hafızasına alır. Kaldırılan birçok dosyaya ve bilgiye bu siteden ulaşılabilir.

**Robtex:**

IP ve domain araştırmalarında kullanılır. Araştırmamızda IP, domain, dns ve routerlar hakkında detaylı bilgiye ulaşabiliriz.

**RIPE NCC & ARIN & APNIC:**

IP adresi ile sorgu yaparak hedefin IP aralıklarını elde etmemizi sağlar. IP sorgularımızda Amerika için ARIN, Avrupa için RIPE, Asya için ise APNIC kullanırız.

**Wappalyzer:**

Sitelerin hangi yazılımları ve teknolojileri kullandığı hakkında bilgi sahibi olabiliriz.

**Aktif Bilgi Toplama**

Pasif bilgi toplama işleminden sonra aktif bilgi toplama işlemi gerçekleştirilir. Aktif bilgi toplama hedef ile direkt olarak temasa geçilerek gerçekleştirilen bilgi toplama çeşididir. Bu bilgi toplama çeşidinde hedef sistem üzerinde iz bırakılır. Bilgi güvenilirliği yüksektir.

**Port Tarama:**

Bilgisayar üzerindeki portlar hangi ağ servisinde çalıştığını anlamak için taranır. Buradan hedefin açıklarını öğrenebiliriz.

**Nmap:**

Herhangi bir ağda bulunan cihaza paketler göndererek verilen cevaplar incelenir. Nmap ile ağda tarama yapılarak açık ve kapalı olan portlar incelenir. Ayrıca işletim sistemi, yazılımdaki zafiyetlerin tespiti gibi bilgilere de ulaşabiliriz.

**Zenmap:**

Nmap’in grafiksel arayüzlü halidir.

**SPARTA:**

Taramamızı basitleştirmek ve hızlandırmak için kullandığımız bir araçtır. Komut ve araçları özelleştirerek araştırmamızı ihtiyaçlarımıza göre yapmamızı sağlar.

**DNSenum:**

Bu araçla bir domain’e ait IP adresleri, mail sunucuları, DNS sunucuları, subdomain’leri tespit edilebilir.

**NetCat:**

Bu sistemde backdoor oluşturmak ve sonra oraya bağlantı kurmak amacıyla kullandığımız araçtır. Dosya aktarımı ve port taraması gibi işlemler için kullanılabilir.

**The Harvester:**

Hedef sistem üzerindeki mail adresleri, alt alanları (subdomain), açık portları bulmak için kullandığımız araçtır.

**Metagoofil:**

Birçok dosya formatını (jpg, pdf, vb.) tarayarak bu dosyalar hakkında bir çok bilgi edinebileceğimiz araçtır.

**SEDANUR SARIKOÇ**