|  |
| --- |
| ***Bilgi Toplama*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ*  Pentesting adımlarından ilk’i olan Bilgi Toplama araçları hakkında bilgi vereceğim. |
| -**Archive-theHarvester**  -**Dig**  -**Dirb**  -**Gobuster**  -**Dmitry** |

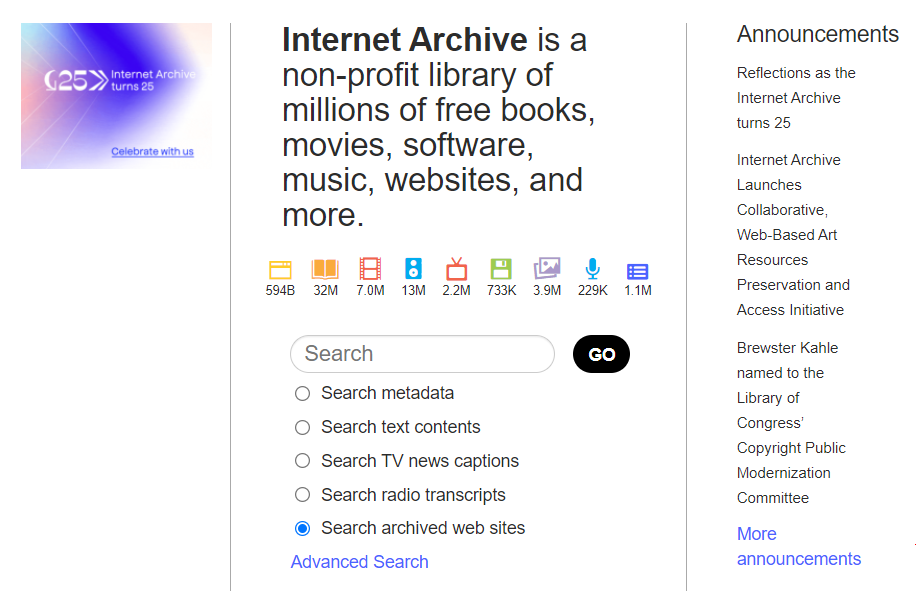
**08.08.2021**

-Bilgi toplama pasif ve aktif bilgi toplama olmak üzere ikiye ayrılmaktadır.

-“Archive.org” sitesinden Pasif bilgi toplama ile başlayalım.

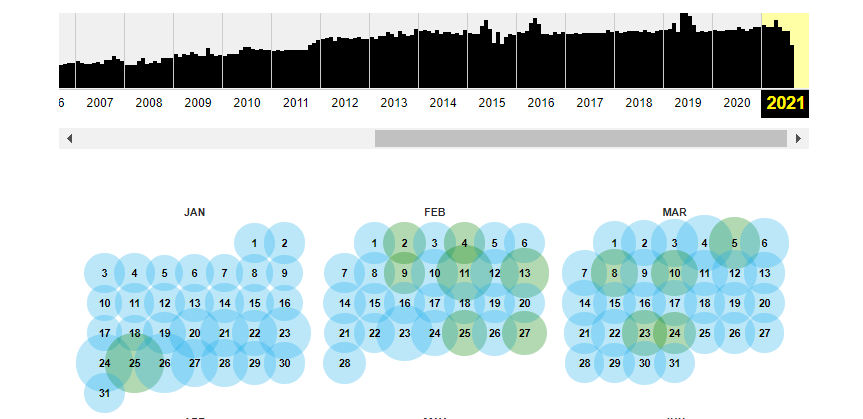
***Archive.org***

-Tarayıcımı açıyorum ve burada "Archive.org" sitesini görüntülüyorum.

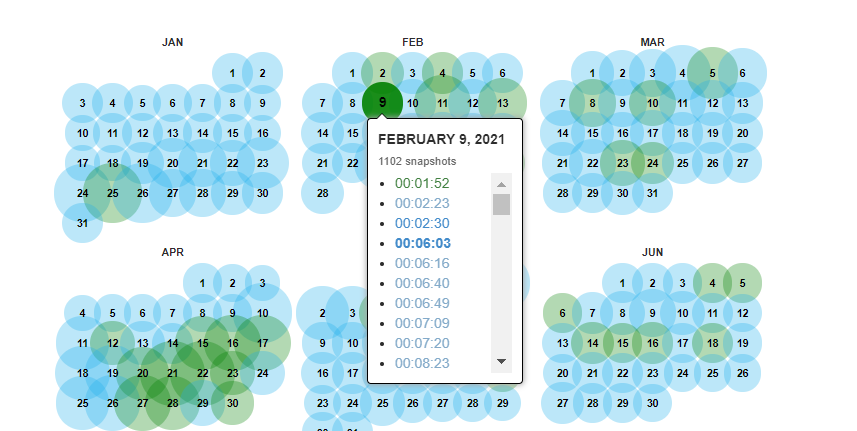


- Siteyi görüntülediğimde karşıma böyle bir ekran geliyor.Burada geçmişe dair saati ve saniyesine kadar değişimini görmek istediğim adresi yazıyorum.

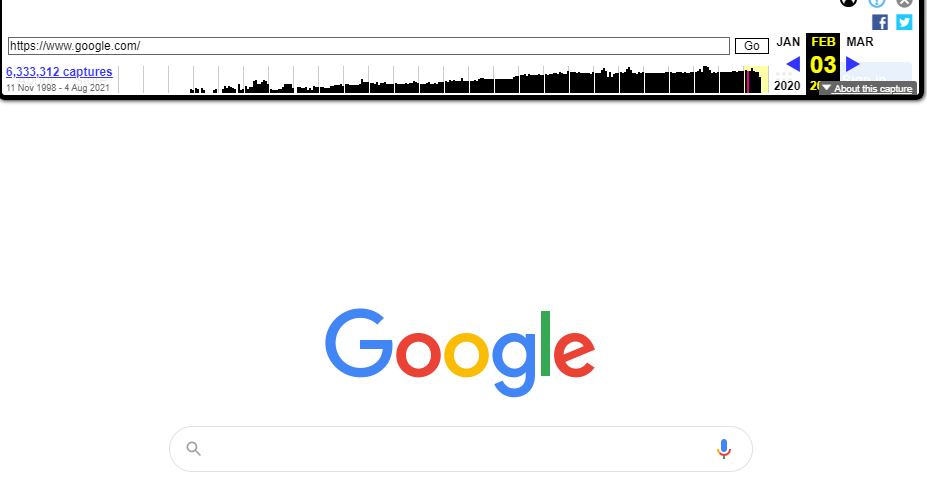
-Google sitesi üzerinden işlem gerçekleştiriyorum.



-Google sitesini görüntülediğimde bana “Google” sitesinin zamana bağlı olarak değişimini gösteriyor.



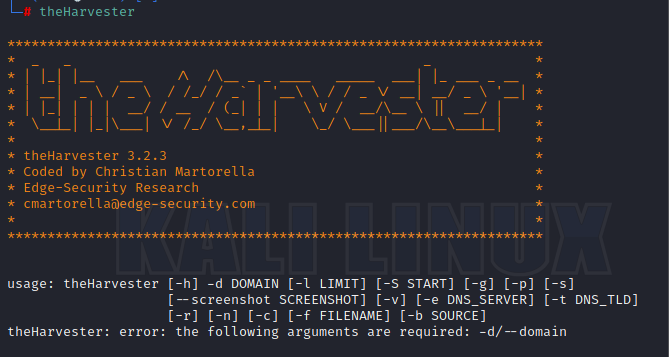
- Burada bir tarih ve saat seçiyorum ve tarayıcı üzerinden görüntülüyorum.



- Google sitesinin o tarihlerde kullandığı uygulamaları,arka planı veya sürümünü bu şekilde görsel olarak görüntüleyebiliyorum.

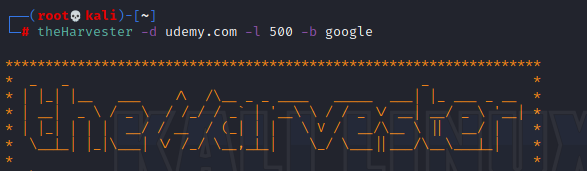
***TheHarvester***

-Bu araç Kali linux üzerinde kurulu olarak gelmektedir.



- Linux üzerinden uçbirimi açıyorum ve burada theHarvester komutu ile çalıştırıyorum.

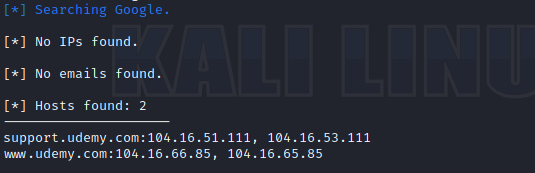
-Bu komut sonrasında bana kullanımıyla ilgili gerekli bilgilendirmeyi yapacaktır.



-“-d” komutu ile tarama yapılacak web sitesini belirtiyorum.

-“-l” Kaç adet arama işlemine bakılacağını belirtiyorum.

-“-b” Kullanılacak arama motorunu belirtiyorum.

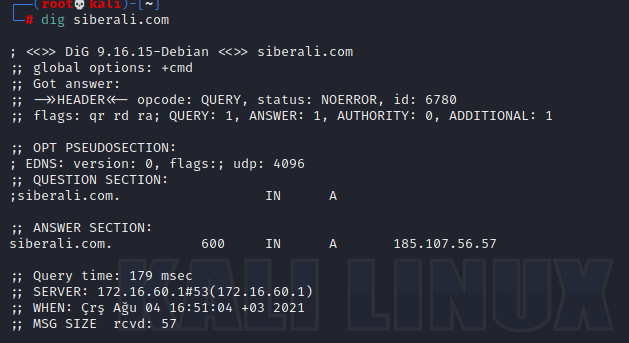


- Burada alt domain isimlerine ve kullanmış olduğu mail adresleriyle ilgili bilgi döndürecektir.

-Alt domainler üzerinden kullanıcı adı ve şifre giriş ekranları default olarak kalır ise bu bir zafiyettir. Burada rahat bir şekilde “Brute Force” yapabiliriz.

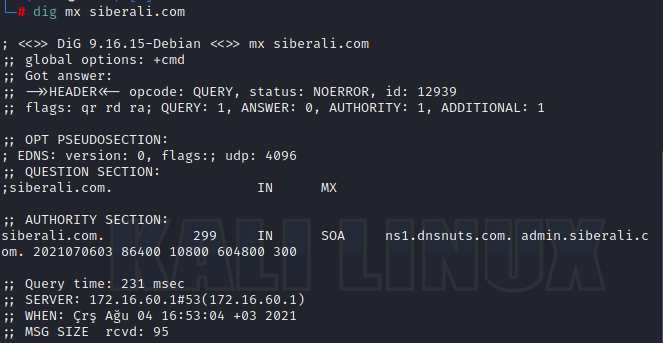
***DİG***

-Alan adı sorgulaması,mail sorgulaması DNS zone transfer açığı sorgulanabilir

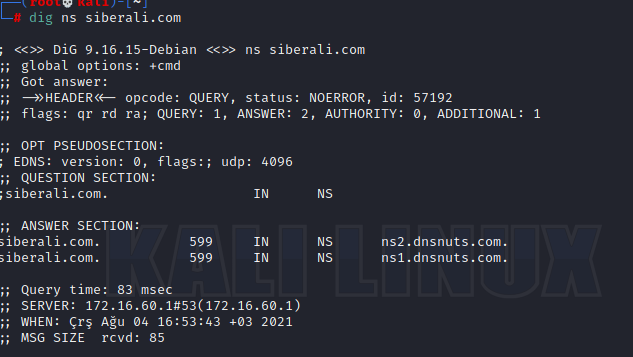


- dig "domain-name" formatı ile çalışmaktadır.Çok basit bir kullanımı vardır.

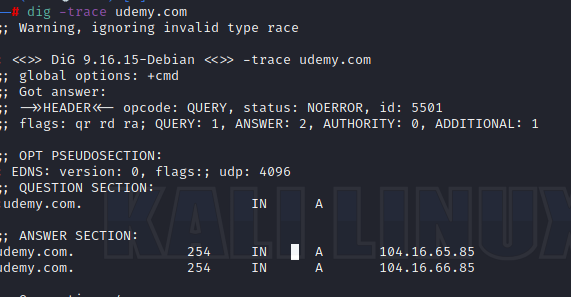
-Bu işlem sonrasında sunucunun IP numarasını görüntüleyebiliyoruz.



-Hedefin mail sunucularını tespit etmek için "dig mx" komutunu kullanıyoruz.



-Alan adından sorumlu “dns” sunucusunu öğrenmek için ise "dig ns" komutunu kullanıyoruz.

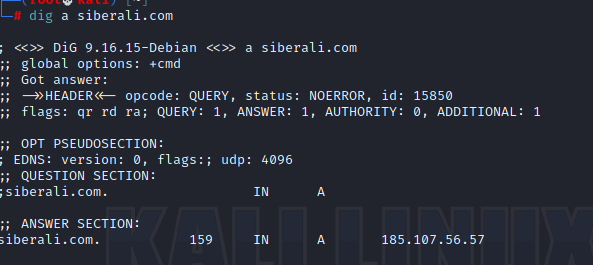


-DNS arama serüvenini görüntülemek için "dig trace" komutunu kullanıyoruz.

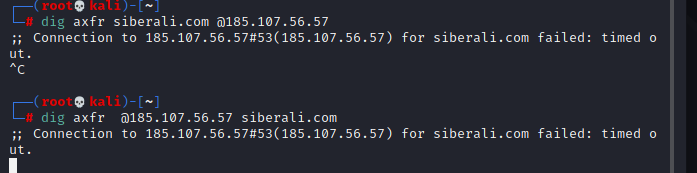
-Burada DNS Zone Transfer açıklığını bulmaya çalışacağız.

-Güvenlik önlemi alınmazsa tüm adres kayıtlarına erişim sağlanabilir.Bilgi çalınma işlemi çok rahat bir şekilde yapılabilir.

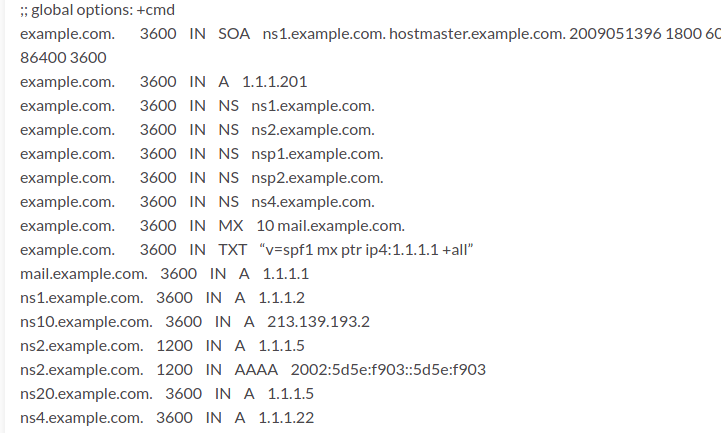
-"dig axfr" komutu ile çalıştırıyoruz. @DNS sunucusunu IP adresini yazıp işlemi başlatacağız.



-Öncelikle sunucunun IP adresini öğreniyorum.



-Bu şekilde bir geri dönüş olur ise sitenin bu alanda açığı olmadığını öğreniyoruz.



-Eğer açık olsaydı nasıl bir geri dönüş olacağını göstermek istiyorum.Network üzerinden bir örnek aldım.

-DNS ZONE işlemi yük eşitlemek için kullanılmaktadır.

***Dirb***

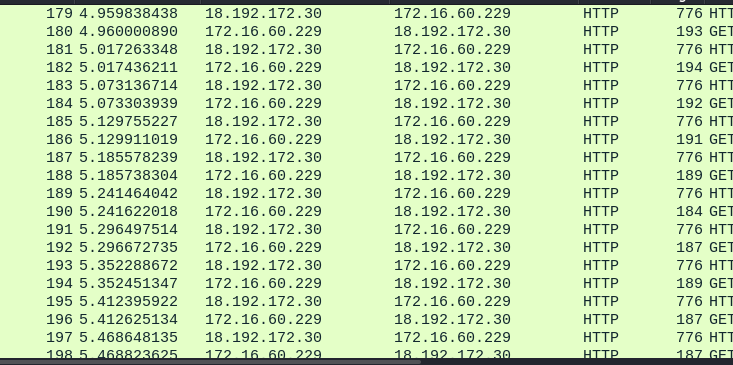
­-Dirb aracı dizin tarama işlemi için kullanılmaktadır.

-Pentesting işlemlerinde sıkça kullanılmaktadır.

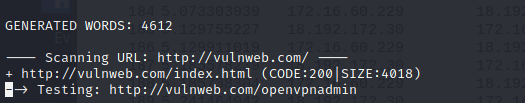
-Böyle basit bir çalışma mekanizması vardır.



-Bruteforce çalışması ile sürekli link denemesi yapılmaktadır.



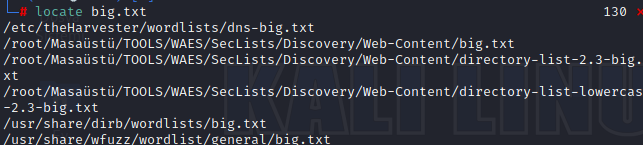
-“Wireshark” üzerinden akışlar baktığım zaman sürekli olarak link denemesi yaptığını görüntüleyebiliyorum.



-Denemiş olduğu “Bruteforce” ataklarının döndürdüğünü hata mesajlarını bize göstermektedir.

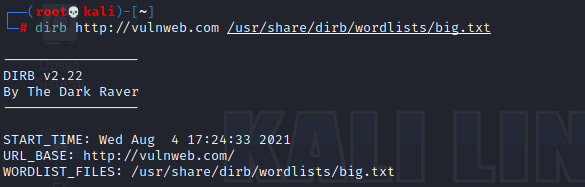
-Hata mesajları üzerinden bir Bypass işlemi gerçekleştirilebilir.

-200 hatası döndürdüğüne bize yazdırıyor.



-Eğer farklı bir Wordlist ile işlem gerçekleştirmek ister isek buna da olanak sağlamaktadır.

-Öncelikle linux üzerinde hazır olarak bulunan “locate” komutu ile bir .txt buluyorum.



- Yazmış olduğum komut ile eklediğim “Wordlist” üzerinden işlemi başlatabiliyoruz.

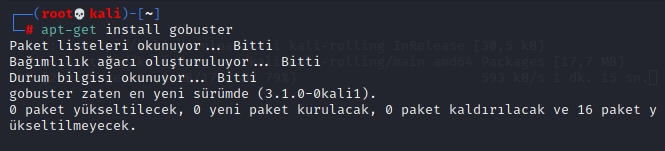
***GoBuster***

-Bu araç Linux üzerinde sürüme bağlı olarak kurulu olarak gelmeyebilir.

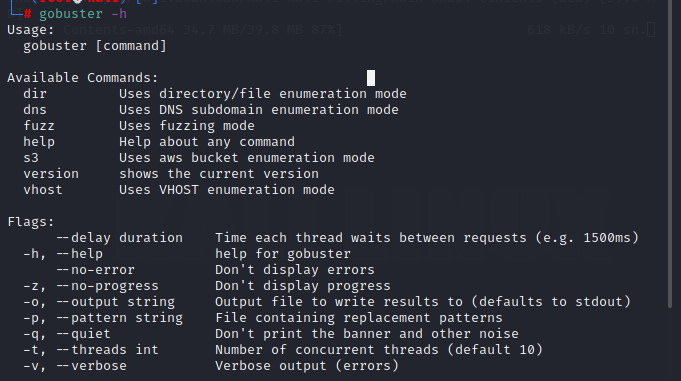
-“Gobuster” ile “dirb” arasında ki fark Gobuster dirb’e göre çok çok daha hızlıdır.

-Dirb bulduğu dizinler arasında arama yaparken, Gobuster yüzeysel bir şekilde geçmektedir.

-Bu işlem öncesinde “apt-get update&upgrade” işlemlerinin gerçekleştirilmesini tavsiye ederim.

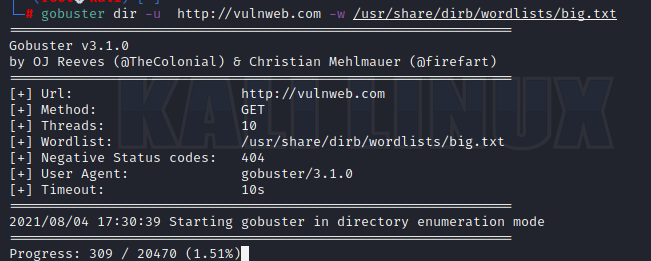


-Apt-get komutu ile kurulum işlemini gerçekleştiriyorum.



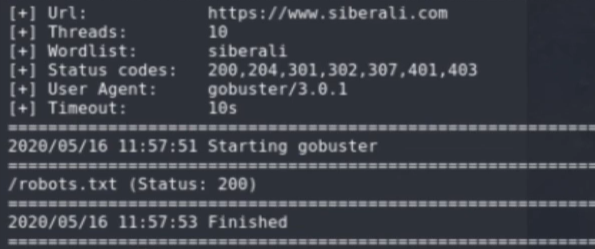
-“Gobuster –h” komutu ile kullanılabileceğimiz komutları görüntüleyebiliyoruz.

-Dizin tarama işlemi başlamış bulunmaktadır

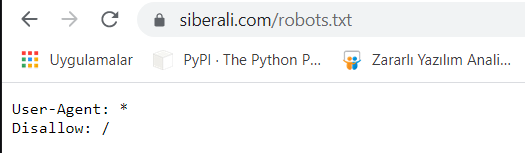


-“-u” parametresi ile tarama yapacağımız Web siteyi belirtiyorum.

-“-w” parametresi ile Wordlist’imi belirtiyorum.



-Vulnweb üzerinden bir açık bulamadığı için başka bir site üzerinden işlemi tekrardan gerçekleştirdim.Burada bulduğu açığı görüntülüyorum.

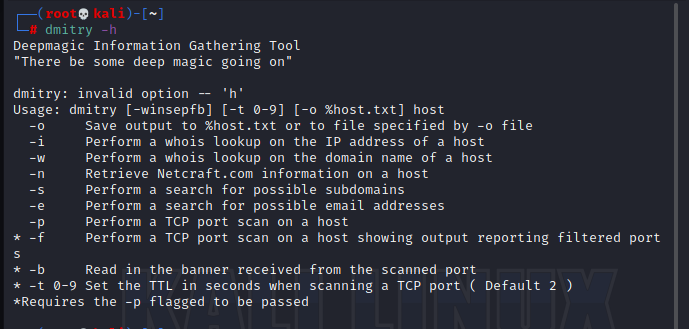


-Robots.txt açığını buldu burada açığı görüntülediğimde bana bilgiler döndürdüğünü görüntülüyorum.

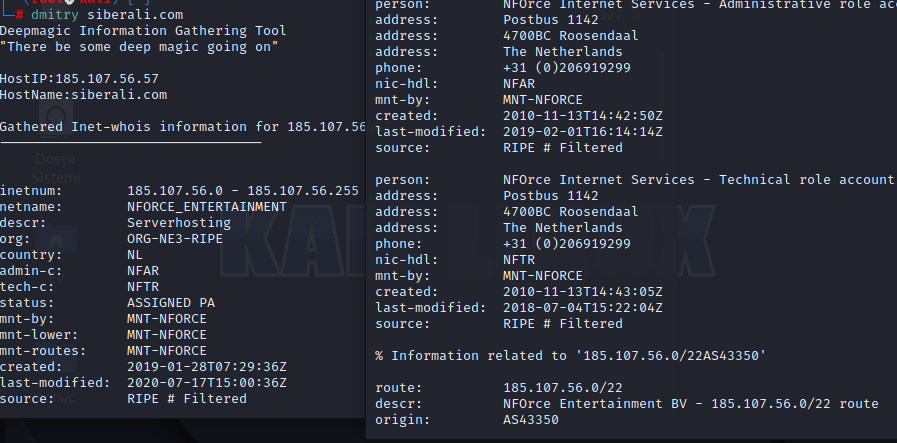
-Bununla ilgili uygulamalar yapılacağı için burayı atlıyorum.

***Dmitry***

-Açık port,IP adresi gibi bilgileri bize sunan bir araçtır.



-"Dmitry -h" komutu ile kullanımı hakkında bilgi elde edebilirim.



-"siberali.com" sitesine bir keşif gönderdiğimde bana döndürdüğü bilgiler bu şekilde görüntüleyebiliyoruz.

-Burada hosting firması hakkında bile bilgi elde edebiliyoruz.



-Aynı şekilde Port taraması da gerçekleştirmektedir fakat bu işlem için Nmap aracını kullanacağız.

-Ayrıca burada DNS server IPlerine de erişim sağlayabiliriz.Bu elde etme işlemi sonucunda buraya yapılacak bir DDOS saldırısı ile servis dışı bırakılabilir.

-Harici olarak “Wireshark” kullanarak analiz işlemi de gerçekleştirilebilir.