**Paket Dinleyici**

**Projesi**

**Hazırlayanlar : İbrahim DEMİRCİ - Ömer Faruk BAHAR**

**Ders : Bilgisayar Ağların Giriş**

**Sorumlu Öğretim Üyesi : Eyüp Emre ÜLKÜ**

**Paket Dinleyici Projesi**

**Proje İçeriği**

Projede bir ağ üzerindeki paketleri izlemek amaçlandı ve benzer bir program olan Wireshark tarzı bir program geliştirdik.

Proje içerisinde sanal bilgisayar ile aynı ağda iken bilgisayarın gönderdiği paketlerin üzerimizden geçmesini sağlayarak gelen giden tüm paketleri ve içeriklerini görüntüledik.

Daha sonra görüntülediğimiz HTTP paketleri içerisinde username ve password başlığında iletilen bilgilere erişim sağladık.

**Projede Kullanılan Teknolojiler ve Platformlar**

* Python
* Scapy
* Kali Linux işletim sistemi olan bir bilgisayar
* Windows işletim sistemi olan bir sanal bilgisayar

“””İkinci bir işlem olarak https olarak çalışan web sayfalarında bilgiler şifrelendiği için bu siteleri birkaç işlem uygulayarak http sayfası formatına çevirip bilgilere erişim sağlıyoruz.

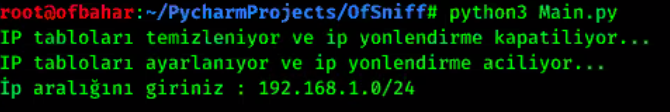
**Gelen giden paketleri nasıl izleriz ?**

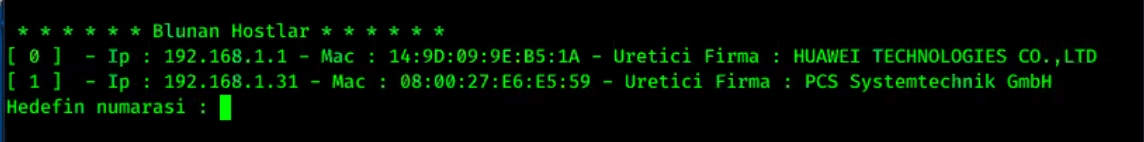
Modem ile istemci bilgisayar arasına girerek bilgisayar bir modemmiş gibi modeme ise o bilgisayarmışız gibi rol yaparak ikisi arasında gerçekleşecek tüm transferlerin bizim üzerimizden geçmesini sağlayarak her detayı görebilir hale geliyoruz.

**Programın Çalışma Aşamaları**

Proje ana hatları ile üç kısımdan oluşuyor. Bunlar **ağ tarama** , **cihaz ile modem arasına geçme** ve **paket dinleme** aşamaları.

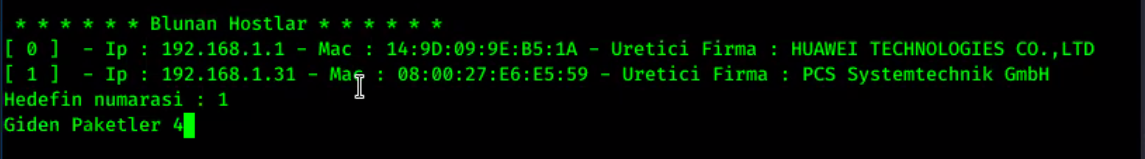
İlk aşamada ip girdisi alıyoruz ve bu aralıkta bulunan cihazları arıyoruz. Cihazlar arandığında IP adresi, MAC adresi ve hangi marka olduğu ekranda görüntülenmekte. (Görsel 1)

İp ekranı ve görünen cihazlar.



İkinci aşamada iki cihaza (modem ve hedef cihaz) arp paketleri göndererek araya geçiyoruz.

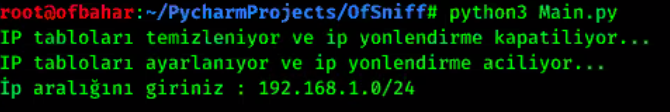
Arp : Adres Çözümleme Protokolü (ARP), Internet Protokolü adresinin (IP adresi) yerel ağda tanınan fiziksel makine adresine eşlenmesi için kullanılan bir protokoldür.

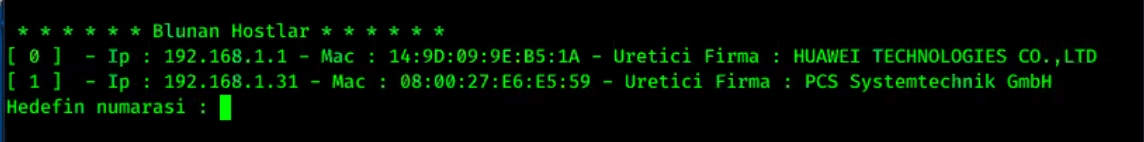


Paketleri görüntüledikten sonra programımızda 80 portunda ile çalışan HTTP paketleri üzerine yoğunlaştık. HTTP paketinde sırasıyla **Raw** katmanı altında **load** bölümünde bulunan veriye filtreleme yoluyla ulaşarak giden username ve password bilgilerini ele geçirme işlemini gerçekleştirdik.

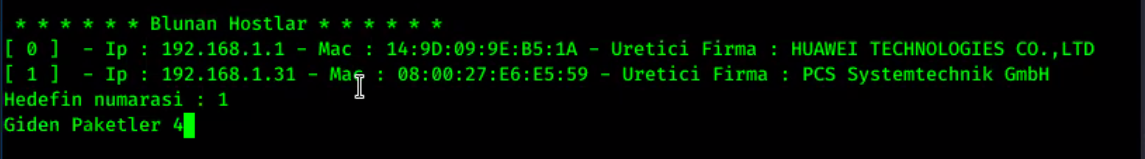
**HTTP Siteler İçin Örnek Deneme :**

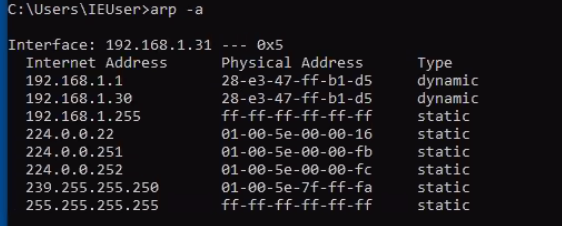
1. İlk önce programımızı çalıştırıyoruz ve bir IP aralığında ağda gerekli taramayı yaptıktan sonra hedef cihazı seçiyoruz.



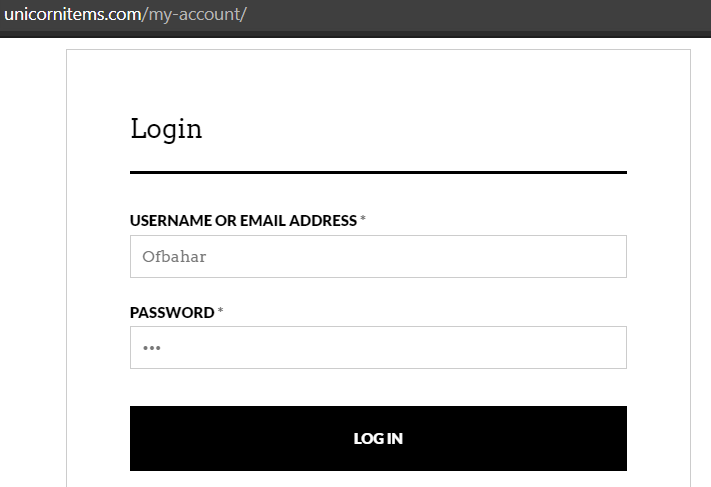


1. Hedef cihaza arp paketleri gönderilirken hedef bilgisayarın komut ekranında arp – a komutu ile etkileşimde olan cihazları görebiliriz.





1. Daha sonra **HTTP** sitede bir form gönderme denemesi yapıyoruz. HTTP paketlerine yapılan filtreleme işlemi ile form içerisinde gönderilen username ve password değerlerini terminalimizde görüntüleyebiliriz.

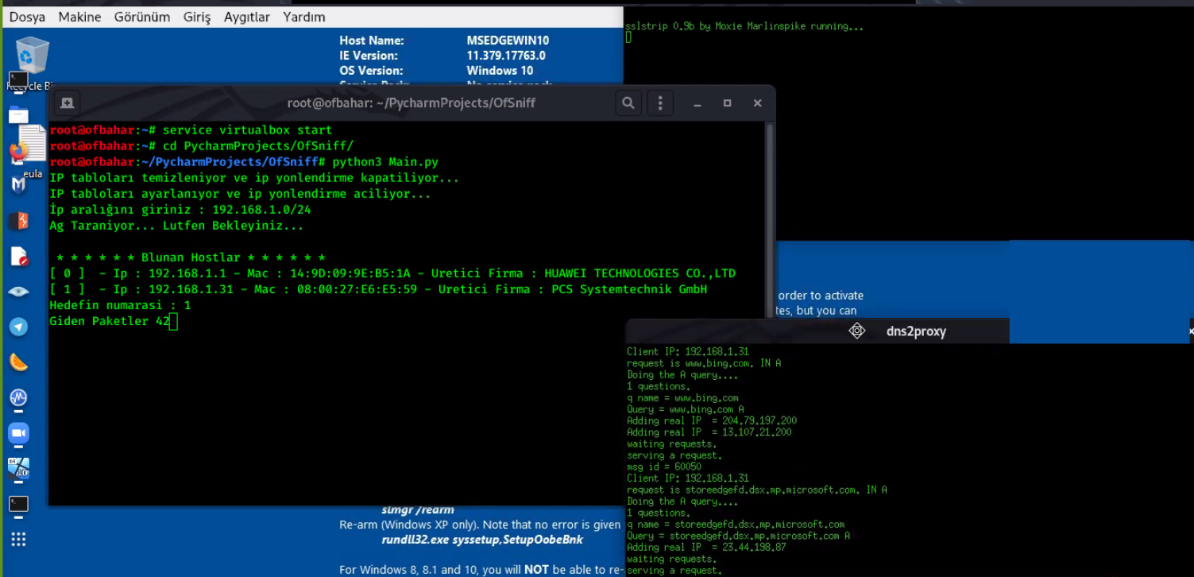




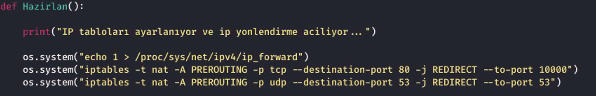
Peki bu HTTP için yapılan işlem **HTTPS** sitelerde de uygulanabilir mi ? Sorumuzun cevabı evet fakat her zaman değil. Bazı web siteleri sslstrip adı verilen bir Proxy yapısı kullanılarak HTTPS 🡪 HTTP dönüşümü yapılarak içerisindeki bilgilere ulaşılabiliyor.

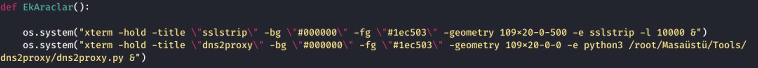
**HTTPS Siteler İçin Örnek Deneme :**

1. HTTP de yaptığımız 1 ve 2. Adımı tekrarlıyoruz ve cihaz ile modem arasında yerimizi alıyoruz.
2. Daha sonra paketler arka planda gönderilirken HTTPS bir web sitesinden form doldurma denemesi yapıyoruz. Bu işlemler yapılırken arka tarafta sslstrip ve dns2prpxy yapıları da çalışır durumda bekliyor.  
   **SSLstrip :** HTTPS siteleri HTTP hale dönüştürmek için çalışan bir Proxy. Bu hizmeti kullanmak için 80 portundaki verileri 10000 portuna yani sslstrip çalışma portuna yönlendirmelerini IPTABLE ayarlamaları ile yapıyoruz.  
   **dns2proxy :** Yine HTTPS 🡪 HTTP dönüşümüne yardımcı bir yapı.

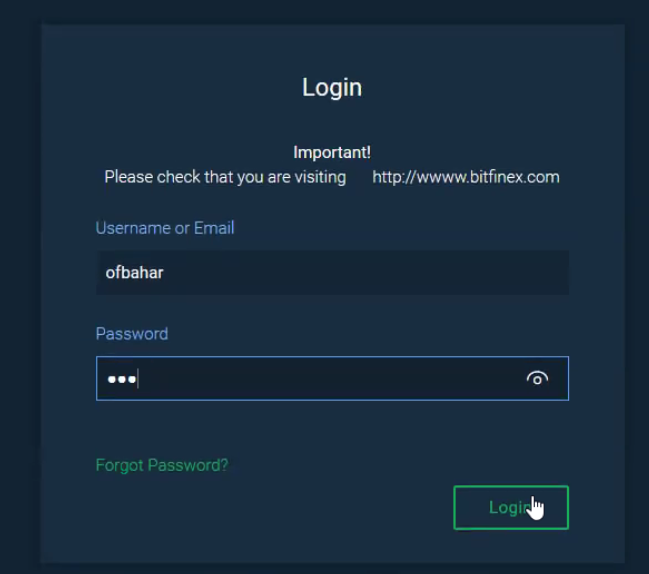


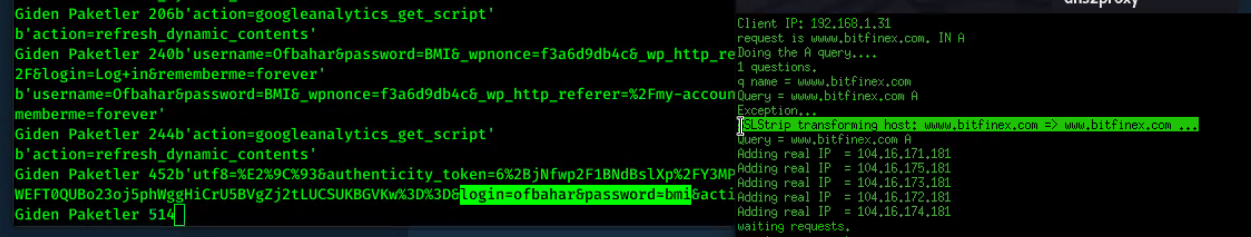
**NOT**: dns2proxy, sslstrip çalıştırma ve iptable ayarlamaları için yazılmış fonksiyonlar aşağıdaki gibidir.





1. Daha sonra **HTTPS** sitede bir form gönderme denemesi yapıyoruz. HTTP paketlerine yapılan filtreleme işlemi ile form içerisinde gönderilen username ve password değerlerini terminalimizde görüntüleyebiliriz.





**Güvenli Site Yok mu ?**

**HSTS** siteler korumalı olarak çalışmaktadır yani HTTPS dışında açılmamakta. Facebook, gmail gibi siteler bunu kullanıyor.

**Bu Durumdan Korunmak İçin Yapılması Gerekenler**

* Kafe, restoran gibi yerlerdeki açık ağlara girmiyoruz.
* Zorunda isek de VPN kullanırız.
* HTTPS sitelerde durmaya devam ediyor olduğumuzu kontrol ediyoruz.
* Şüphelenirsek de arp -a yaptığımızda IP ve MAC ve etkileşim cihazlarını da görebiliriz.