



**KAHRAMANMARAŞ SÜTÇÜ İMAM ÜNİVERSİTESİ  
MÜHENDİSLİK VE MİMARLIK FAKÜLTESİ  
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ  
BİLGİSAYAR VE AĞ GÜVENLİĞİ PROJE ÖDEVİ**

**DNS SPOOFING**

**Onur Yaşar Karaduman, 18110131055**

**Ali Emir, 18110131044**

**2021-2022**

## 1 )PROJENİN AMACI

Saldırılacak olan hedef cihazın DNS ön belleğine erişim elde ederek gerçek girilecek olan bir sitenin IP adresini sahte bir web sitesinin IP adresiyle değiştirerek kullanıcının gerçek web sitesi yerine dolandırıcılık için hazırlanan sahte web sitesine yönlendirme işlemi yapılacaktır. Bu saldırı biçiminde dns kayıtları değiştirilerek yapılacaktır.

### Kullanılacak olan işletim sistemi ve yazılımlar

**Kurban:** Windows 10

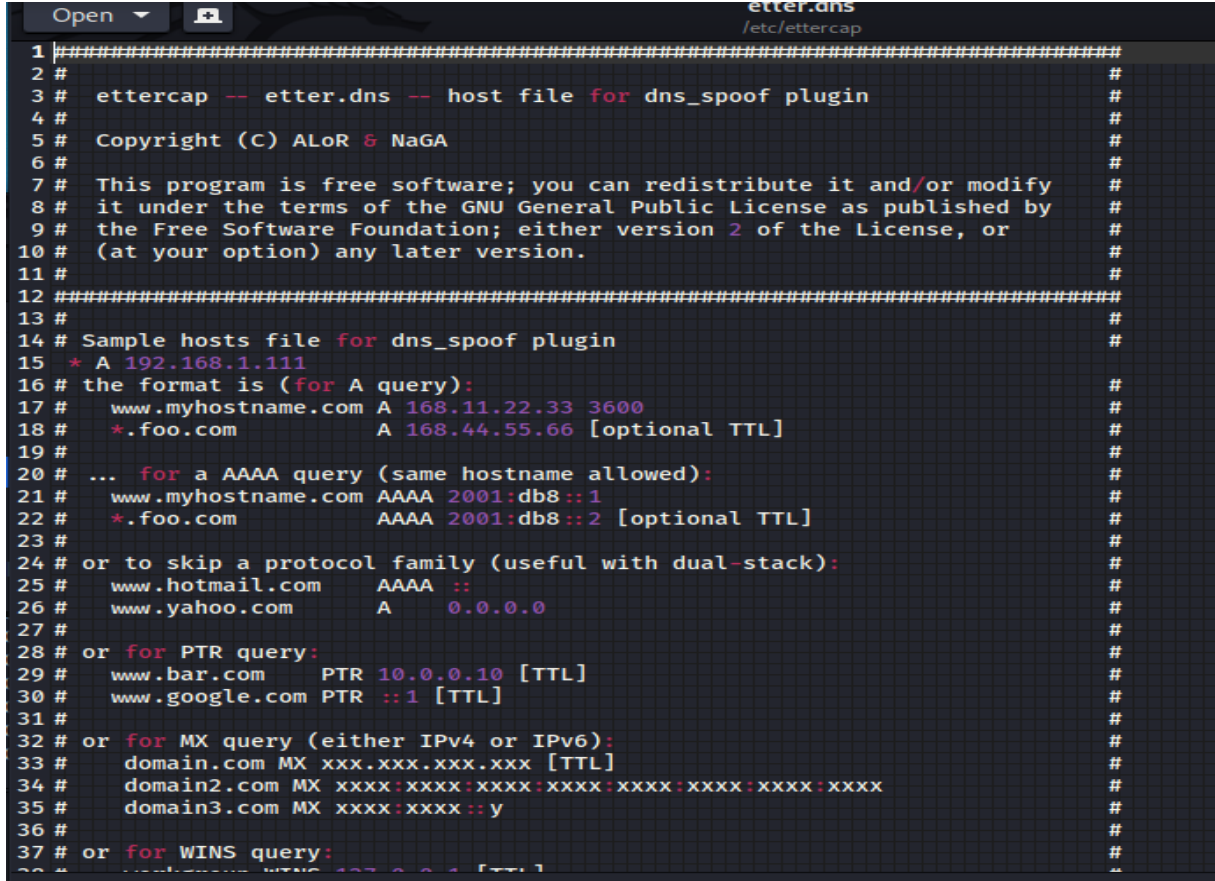
**Saldırgan:** Kali Linux

**Kullanılacak Olan Araç:** Ettercap

Projemiz kişisel bilgilerin yetkisiz kişilerin eline geçmesini sağladığı için bilgi güvenliği temel unsurlarından **Gizlilik** , saldırılan cihazın gerçek siteye olan erişimini engellediği için ise **Erişilebilirlik** unsurlarını ihlal etmektedir.

## 2) PROJENİN GERÇEKLEŞTİRİLMESİ

Kali linuxu açıyoruz ve kablosuz ağa bağlanıyoruz. Daha sonra kurbanı yönlendirilmesini istediğimiz ip değerini giriyoruz. Çünkü kurbanın herhangi bir web sayfasını açtığında yönlendireceği ip Şekil 1’ de bulunan 192.168.1.111 ip değeridir.



```
1 #####
2 #
3 # ettercap -- etter.dns -- host file for dns_spoof plugin
4 #
5 # Copyright (C) ALOR & NaGA
6 #
7 # This program is free software; you can redistribute it and/or modify
8 # it under the terms of the GNU General Public License as published by
9 # the Free Software Foundation; either version 2 of the License, or
10 # (at your option) any later version.
11 #
12 #####
13 #
14 # Sample hosts file for dns_spoof plugin
15 # * A 192.168.1.111
16 # the format is (for A query):
17 #   www.myhostname.com A 168.11.22.33 3600
18 #   *.foo.com          A 168.44.55.66 [optional TTL]
19 #
20 # ... for a AAAA query (same hostname allowed):
21 #   www.myhostname.com AAAA 2001:db8::1
22 #   *.foo.com          AAAA 2001:db8::2 [optional TTL]
23 #
24 # or to skip a protocol family (useful with dual-stack):
25 #   www.hotmail.com    AAAA ::
26 #   www.yahoo.com      A    0.0.0.0
27 #
28 # or for PTR query:
29 #   www.bar.com        PTR 10.0.0.10 [TTL]
30 #   www.google.com     PTR ::1 [TTL]
31 #
32 # or for MX query (either IPv4 or IPv6):
33 #   domain.com MX xxx.xxx.xxx.xxx [TTL]
34 #   domain2.com MX xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
35 #   domain3.com MX xxxx:xxxx::y
36 #
37 # or for WINS query:
38 #   domain.com WINS 192.0.0.1 [TTL]
```

Şekil 1

Ettercap aracının kullanıcı arayüzünü çalıştırmak için terminal’de “ettercap -G” komutunu çalıştırıp, uygulama çalıştıktan sonra saldırıyı gerçekleştireceğimiz primary interface’ini (birincil arayüz) seçmemiz gerekmektedir. (Şekil 2)



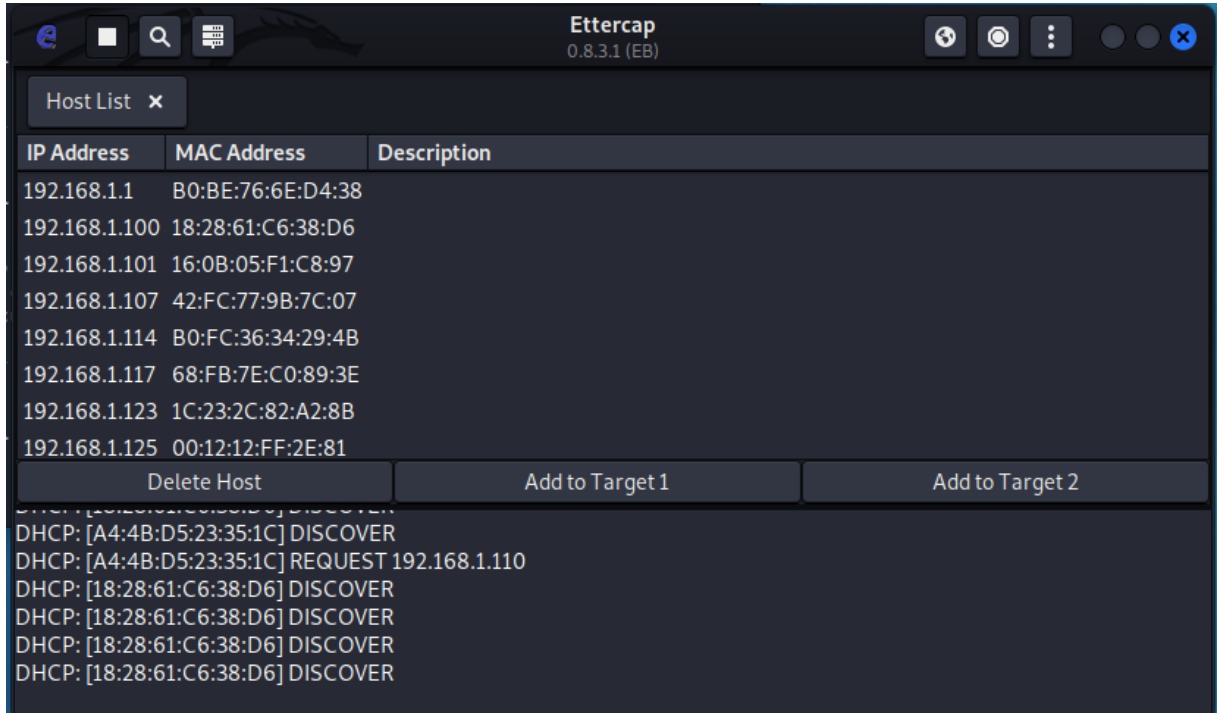
Şekil 2

“Hosts” sekmesindeki “Scan for Hosts” seçeneğini seçerek bulunduğumuz primary interface üzerinde tarama yapabiliriz. 255 tane makine taranıp 20 makinenin hosts listesine eklendiği görülmektedir. (Şekil 3)



Şekil 3

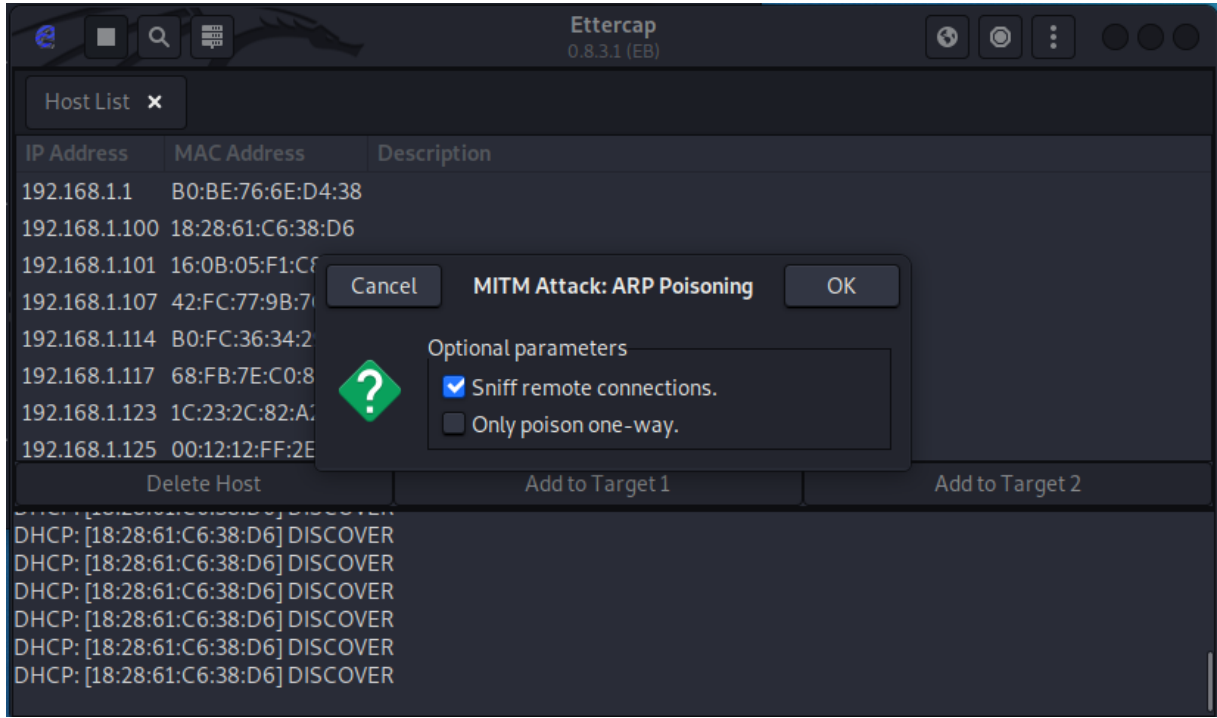
Şekil 3’de tespit edilen 20 tane IP adresini görüntülemek için “Hosts” sekmesindeki “Hosts list” seçeneğini seçmek gerekir. Tespit edilen IP adresleri Şekil 4’de gösterilmektedir.



Şekil 4

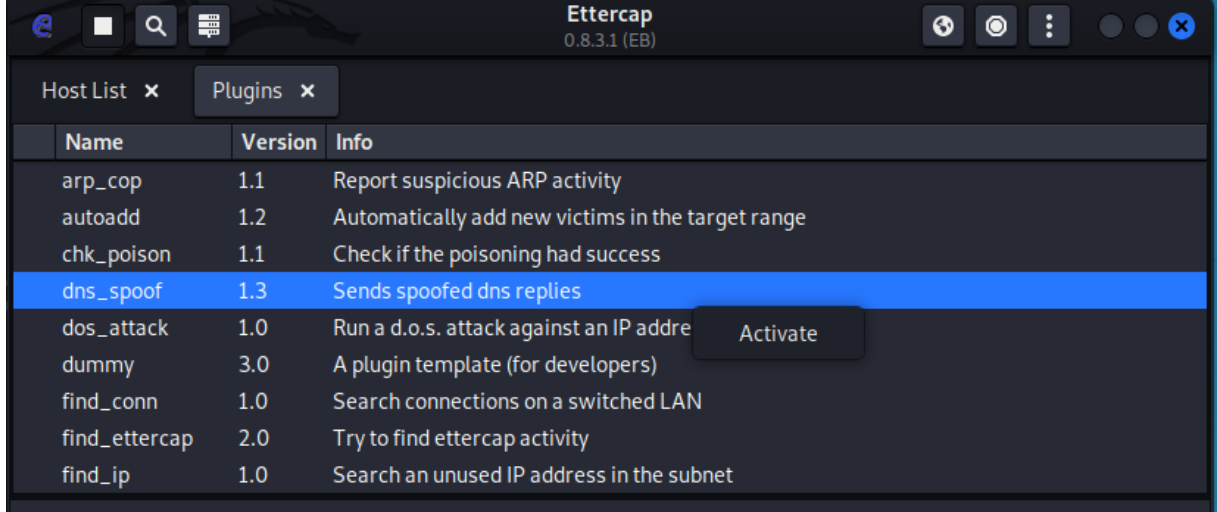
Şekil 4’de kurban IP adresi “192.168.1.134” olarak belirlenmiştir. Belirlenen IP adresini hedef IP olarak belirlemek için IP adresini seçtikten sonra “Add to Target1” butonuna tıklanır. Hedef belirlendikten sonra saldırı başlatılır.

Şekil 4’de kurban IP adresini belirledikten sonra “Mitm” sekmesindeki “ARP Poisoning” seçeneği seçilerek MITM saldırısı başlatılır. Şekil 4’de MITM saldırısı yapmak için beş farklı teknik gösterilmektedir. Bunlardan ARP Poisoning saldırısını yaparak ARP zehirlemesi yapılacaktır. Böylelikle kurban makinesi bir istekte bulunduğunda, istekteki bulunan Destination MAC adresinin biz olduğunu kurban makineye ARP Reply paketi göndererek belirteceğiz. (Şekil 5)



Şekil 5

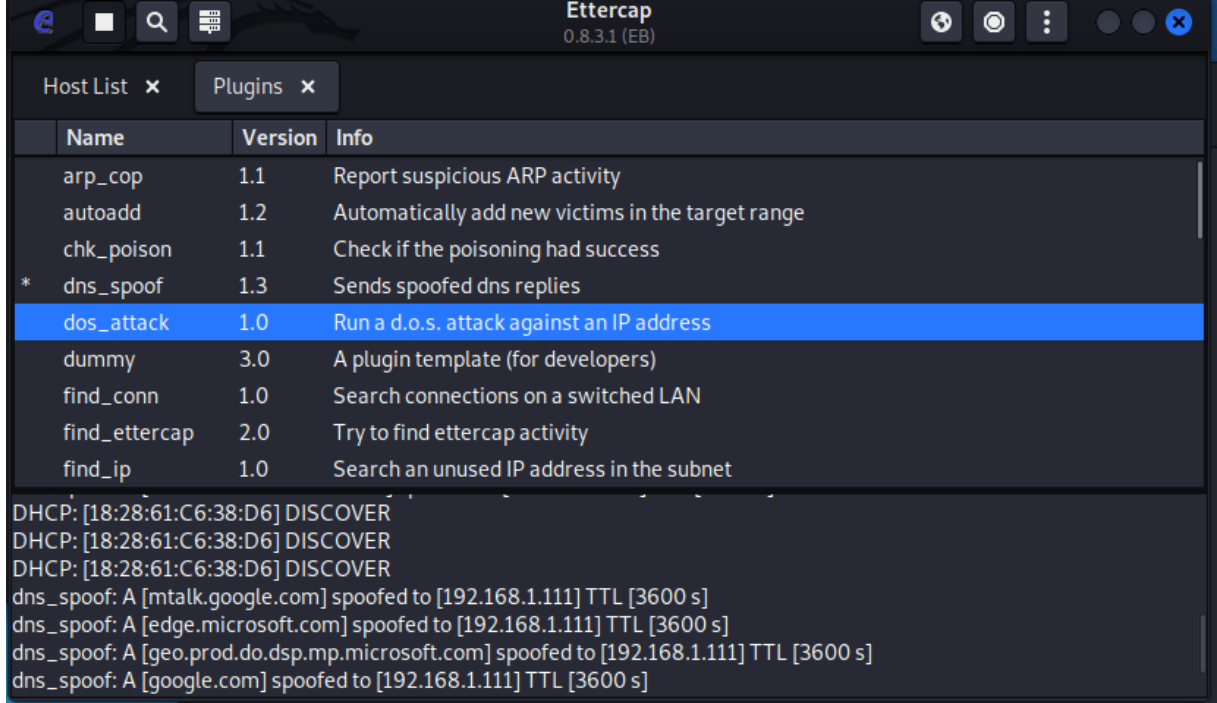
Şekil 6’da MITM saldırısı sırasında DNS Spoofing saldırısı yapmak için “Plugins” sekmesindeki “Manage the plugins” seçeneğini seçerek “dns\_spoof” plugin’ini eklememiz gerekir.



Şekil 6

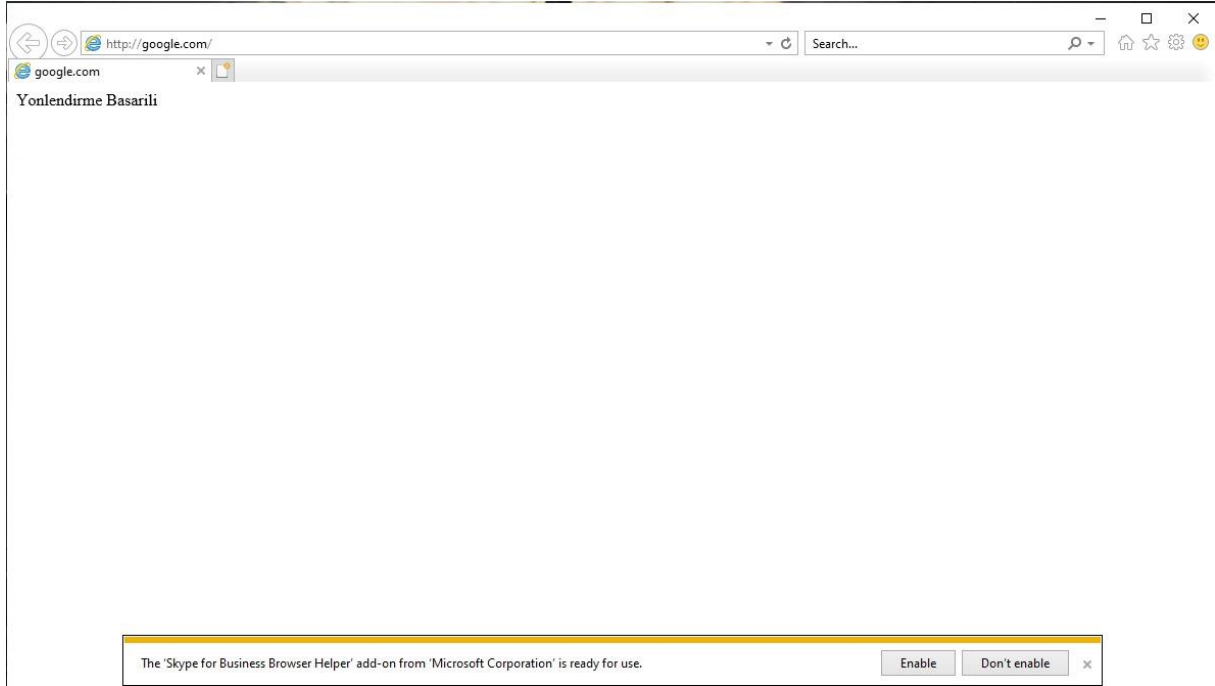


Şekil 7’de “dns\_spoof” eklentisi seçilerek yapılan MITM saldırısı sırasında DNS Spoofing saldırısı başlatılır. Böylelikle, saldırgan DNS Spoofing yaparak kurban makinesinin içerisindeki DNS Cache’te bulunan DNS kayıtlarından Host Record kaydını saldırgan makinesinin IP adresi olarak değiştirecektir.



Şekil 7

Şekil 8’de ise DNS Spoofing saldırısı başarılı bir şekilde gerçekleştirilmiştir. Kurban, saldırgan IP adresine yönlendirilerek, çalıştırılmış olan Apache servisi üzerindeki hazırlanmış olan HTML sayfasını görecektir. Yönlendirme işlemi herhangi bir web sitesine de yapılabilir. Örnek olarak “google.com” domain adresine yönelik yaptığımız bu saldırı, farklı bir domaine yönelik de yapılabilir. Kurban bir facebook kullanıcısı ise, saldırgan sahte bir facebook sayfası oluşturup “etc/ettercap/etter.dns” ayarlarında “facebook.com” domain adresine karşı kötü amaçlı sahte web sitesinin IP adresini verip kurbanı yönelik bir spoofing saldırısını gerçekleştirebiliriz.



Şekil 8

### 3) KAYNAKÇA

- 1- [https://tr.wikipedia.org/wiki/DNS\\_spoofing](https://tr.wikipedia.org/wiki/DNS_spoofing)
- 2- <https://www.kali.org/tools/ettercap/>