



WIFI ATTACK AND DEFENSE

Besim ALTINOK
Security Engineer

MAC Filtrelemesini Aşmak



Pika Pika

Windows Sistemlerde MAC Adresini Öğrenmek

```
cmd Komut İstemi
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\securityci>route PRINT -4
=====
Interface List
14...[redacted]1 .....Realtek PCIe FE Family Controller
 9...[redacted]9 .....Microsoft Wi-Fi Direct Virtual Adapter
18...0a 00 27 00 00 00 .....VirtualBox Host-Only Ethernet Adapter
 2...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
24...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
22...[redacted] .....Broadcom 802.11n Ağ Bağdaştırıcısı
 7...[redacted] .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
11...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
16...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
21...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
17...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
25...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #5
=====

IPv4 Route Table
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface    Metric
```

Windows Sistemlerde MAC Adresini Öğrenmek

```
Windows PowerShell (x86)
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

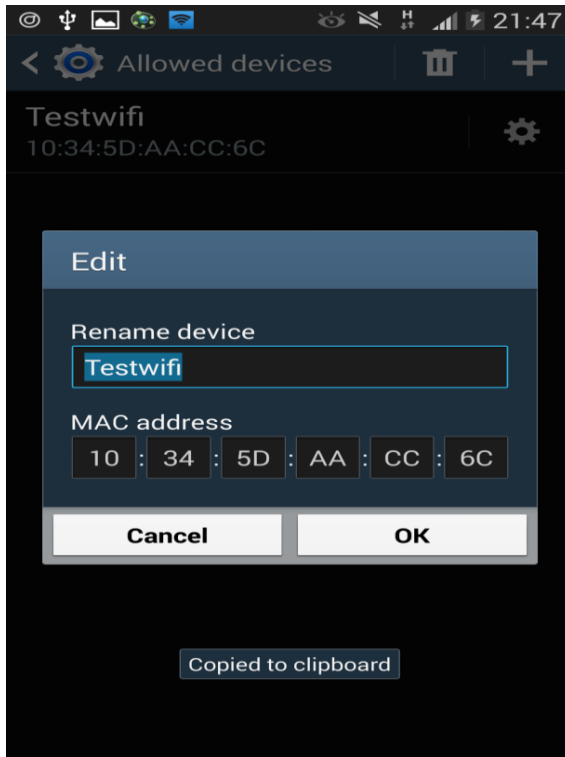
PS C:\Users\securityci> Get-WmiObject win32_networkadapterconfiguration | select description, macaddress

description                               macaddress
-----
Microsoft Kernel Debug Network Adapter
Realtek PCIe FE Family Controller
Broadcom 802.11n Ağ Bağdaştırıcısı      58-26-56-26-10-00
Microsoft Wi-Fi Direct Virtual Adapter  E8-26-56-26-10-00
Microsoft ISATAP Adapter
Microsoft Teredo Tunneling Adapter
WAN Miniport (SSTP)
WAN Miniport (IKEv2)
WAN Miniport (L2TP)
WAN Miniport (PPTP)
WAN Miniport (PPPOE)
WAN Miniport (IP)
WAN Miniport (IPv6)
WAN Miniport (Network Monitor)
Bluetooth Device (RFCOMM Protocol TDI)
Bluetooth Device (Personal Area Network)
VirtualBox Host-Only Ethernet Adapter   0A:00:27:00:00:00
Microsoft ISATAP Adapter
VMware Virtual Ethernet Adapter for VMnet1 00:50:56:C0:00:01
Microsoft ISATAP Adapter
VMware Virtual Ethernet Adapter for VMnet8 00:50:56:C0:00:08
Microsoft ISATAP Adapter
Microsoft ISATAP Adapter
EnGenius 802.11n Wireless USB Adapter
```

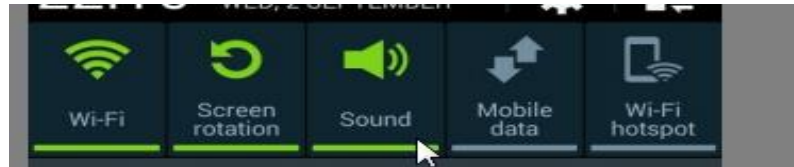
Linux Sistemlerde MAC Adresini Öğrenmek

```
Terminal - securityci@max: ~  
File Edit View Terminal Tabs Help  
~ 23:17:22  
$ ifconfig | grep -i 'HWaddr'  
eth0      Link encap:Ethernet HWaddr C: [REDACTED]  
mon0      Link encap:UNSPEC HWaddr C: 65:15:17:50:83:21-30-00-00-00-00-00-00-00  
wlan0      Link encap:Ethernet HWaddr C: [REDACTED]  
~ 23:17:30  
$
```

MAC Filter Bypass İçin LAB Kurulumu



- Bu aşamadaki testlerimiz için bir cep telefonu kullanacağız ve bu telefondan MAC filtreleme yapıp belirttiğimiz makinelere erişim izni vereceğiz.
- Sonraki adımlarda bu filtrelemeyi aşmak için bazı işlemler gerçekleştireceğiz.



- Bu işlem için wifi özelliğini kapatıyoruz
- Mobil data ve Wifi hotspot özelliğini açıyoruz
- Daha sonra '**Allowed devices [izin verilen cihazlar]**' kısmından filtreleme koyuyoruz.

MAC Filter Bypass İçin LAB Kurulumu

MAC Filtresini aşmak için aşağıdaki adımları izleyeceğiz :

1. İlk olarak MAC Filtrelemesi yapan AP **airodump-ng** ile izlenir
2. AP cihazına bağlı istemcilerin MAC adresleri tespit edilir.
3. Daha sonra bunlardan bir tanesi seçilerek MAC adresini kopyalanır.
4. Bazı durumlarda kopyalanacak MAC adresine sahip istemcinin hattan düşürülmesi gerekebilir.

MAC Filtrelemesini Aşmak - Linux

Mac filtreleme kısmını aşmak için MAC adresimizi değiştirmemiz gerekmektedir. Linux sistemlerde bunun için 3 yöntem mevcuttur.

1. **Macchanger** aracını kullanarak değiştirmek
 - Random değer atamak
 - Özel bir MAC adresi atamak
2. **ifconfig** ile mac adresi atamak
3. **GUI** desteği ile mac adresi atamak

MAC Filtrelemesini Aşmak - Linux

Macchanger aracını kullanarak MAC adresi değiştirme

```
Terminal - bash
File Edit View Terminal Tabs Help
bash securityci@max: ~
securityci@max ~ $ sudo ifconfig wlan0 down
securityci@max ~ $ macchanger -r wlan0
Current MAC: c4:7c:2f:17:17:17 (TP-LINK TECHNOLOGIES CO.,LTD)
Permanent MAC: c4:7c:2f:17:17:17 (TP-LINK TECHNOLOGIES CO.,LTD)
[ERROR] Could not change MAC: interface up or insufficient permissions: Operation not permitted
securityci@max ~ $ sudo macchanger -r wlan0
Current MAC: c4:7c:2f:17:17:17 (TP-LINK TECHNOLOGIES CO.,LTD)
Permanent MAC: c4:7c:2f:17:17:17 (TP-LINK TECHNOLOGIES CO.,LTD)
New MAC: c4:7c:2f:17:17:17 (TP-LINK TECHNOLOGIES CO.,LTD)
It's the same MAC!!
securityci@max ~ $
```

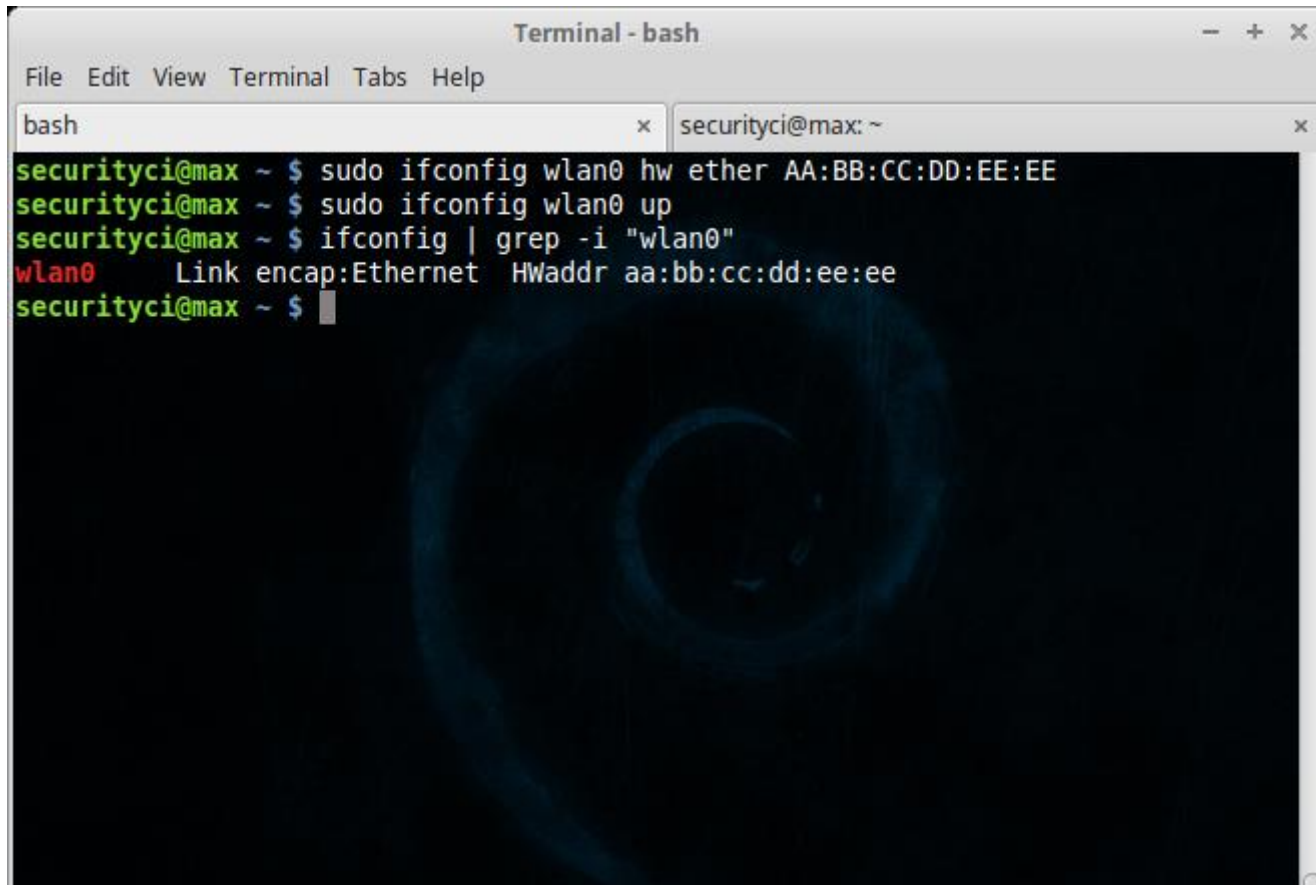
MAC Filtrelemesini Aşmak - Linux

Macchanger aracını kullanarak MAC adresi değiştirme

```
Terminal - bash
File Edit View Terminal Tabs Help
bash securityci@max: ~
securityci@max ~ $ sudo macchanger -m AA:AA:AA:AA:AA:AA wlan0
Current MAC: 08:00:27:00:00:00 (TP-LINK TECHNOLOGIES CO.,LTD)
Permanent MAC: 08:00:27:00:00:00 (TP-LINK TECHNOLOGIES CO.,LTD)
New MAC: aa:aa:aa:aa:aa:aa (unknown)
securityci@max ~ $
```

MAC Filtrelemesini Aşmak - Linux

ifconfig aracını kullanarak MAC adresi değiştirme

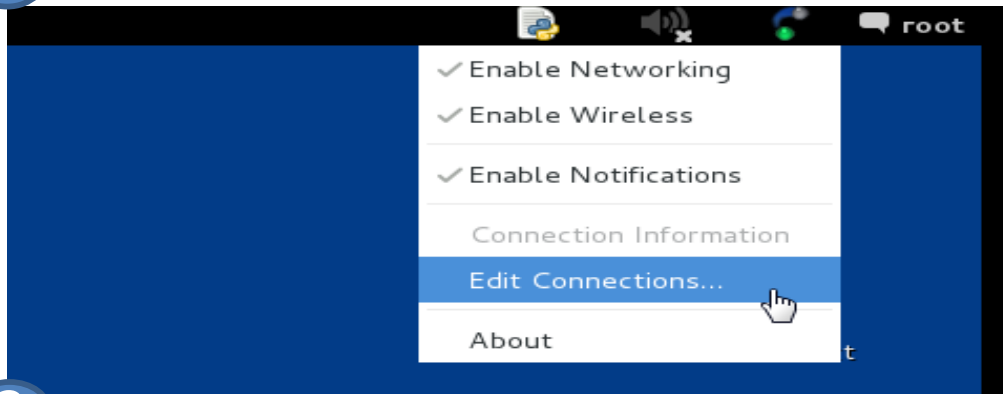
A terminal window titled "Terminal - bash" with a menu bar (File, Edit, View, Terminal, Tabs, Help) and two tabs labeled "bash" and "securityci@max: ~". The terminal shows a series of commands and their outputs: 1. "sudo ifconfig wlan0 hw ether AA:BB:CC:DD:EE:EE" is executed. 2. "sudo ifconfig wlan0 up" is executed. 3. "ifconfig | grep -i 'wlan0'" is executed, resulting in the output "wlan0 Link encap:Ethernet HWaddr aa:bb:cc:dd:ee:ee". 4. The prompt returns to "securityci@max ~ \$".

```
Terminal - bash
File Edit View Terminal Tabs Help
bash x securityci@max: ~ x
securityci@max ~ $ sudo ifconfig wlan0 hw ether AA:BB:CC:DD:EE:EE
securityci@max ~ $ sudo ifconfig wlan0 up
securityci@max ~ $ ifconfig | grep -i "wlan0"
wlan0      Link encap:Ethernet  HWaddr aa:bb:cc:dd:ee:ee
securityci@max ~ $
```

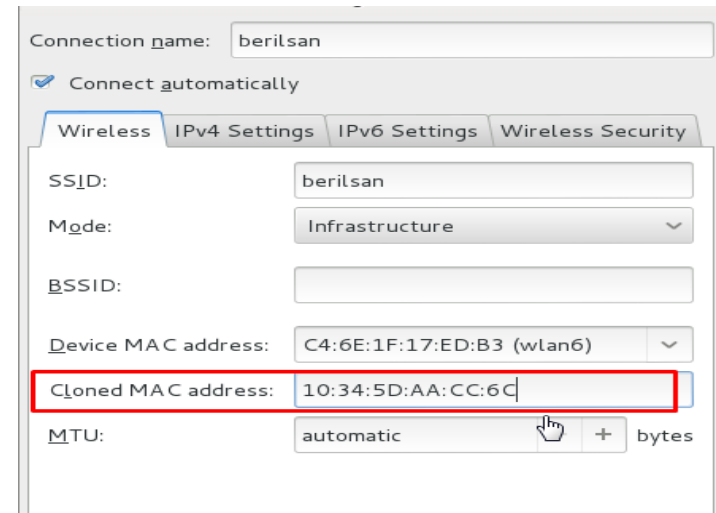
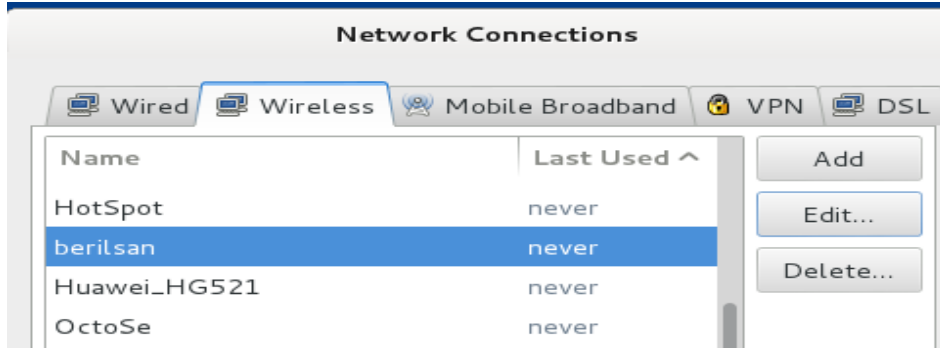
MAC Filtrelemesini Aşmak - Linux

GUI kısmından bir MAC adresi klonlamak

1



2



3

MAC Filtrelemesini Aşmak - Windows

- Windows sistemlerde MAC adresini değiştirmek için 3 farklı seçeneğimiz bulunmaktadır.
 1. Sistem ayarlarından MAC adresi atamak
 2. Regedit ayarlarından MAC adresi atamak
 3. Ek bir yazılım kullanmak

MAC Filtrelemesini Aşmak - Windows

Sistem ayarlarından MAC adresini değiştirmek

