WIFI ATTACK AND DEFENSE

Besim ALTINOK
Security Engineer

Scapy ile Derinlemesine Kablosuz Ağ Analizi

Scapy Hakkında

- Kullanıldığı sistemde Python yüklü olmalıdır.
- Windows ve Linux sistemlerde desteklenmektedir.
- Python ile yazılmış bir kütüphanedir.
- TCP/IP ağlar için özelleştirilmiş paketler üretilebilir.
- Esnek bir yapıya sahiptir. Bu sayede TCP/IP paketlerini dilediğiniz gibi yapılandırabilirsiniz.
- Network taramaları ve analizleri gerçekleştirilebilir.
- Birçok protokole ait paketleri işleyip çözebilir, gönderebilir, yakalayabilir, istek ve cevapları eşleyebilir ve daha fazlasını yapabilir. Tarama (scanning), iz sürme (traceroute), derinlemesine araştırma (probing), birim testleri (unit test), saldırılar (attack) ve network keşfi gibi pek çok klasik işin üstesinden kolaylıkla gelebilir (hping, nmap'in bir kısmı, arpspoof, arp-sk, arping, tcpdump, tethereal, p0f gibi programların yerini tutabilir).
- 356 protokolü destekler.

Scapy Hakkında

Bilmemiz gereken Temel Komutlar:

- ls() komutu ile desteklediği protokolleri görebiliriz.
- lsc() komutu ile kullanabileceğim fonksiyonları görüntüleyebiliriz.
- help(komut) ile komutların kullanımı hakkında yardım alabiliriz.
- conf ile var olan yapılandırma ayarlarını görüntüleyebilir ve değişiklik yapabiliriz.
- sr1() - Layer 3 te paket gönderir ve sadece cevap döndürür.
- sr() - Layer 3 te paket gönderip alabilir.
- send() - Layer 3 te paket gönderebilir
- srloop() - Layer 3 te bir döngüde paket gönderir ve dönen cevapları ekrana basar.

Scapy Hakkında

Scapy Kütüphanesinin Kurulumu

- sudo apt-get install pip
- sudo pip install python-scapy

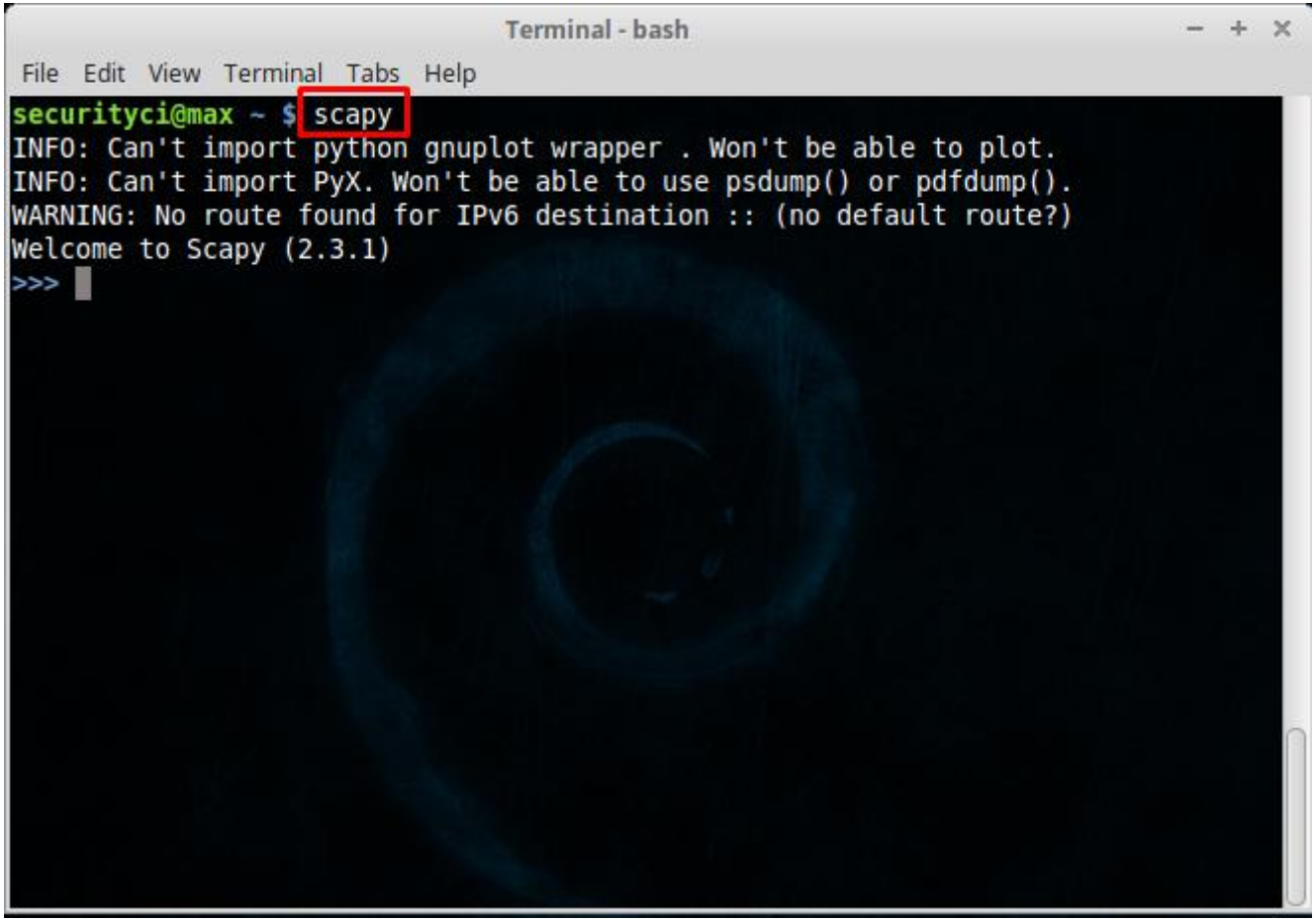
Scapy Kütüphanesinin Python Yazılımlarına Dahil Edilmesi

- from scapy. all import *
  - scapy içindeki bütün fonksiyonları dahil eder.
- from scapy. all import sniff
  - scapy içindeki sadece sniff fonksiyonunu kullanmak için

Scapy ile Adım Adım Kablosuz Ağ Analizi

Kurulumdan Sonra İlk Erişim

İlk erişimi yapmak için Linux sistemden **root** yetkileri ile "**scapy**" yazmamız yeterli olacaktır



Scapy ile Adım Adım Kablosuz Ağ Analizi

Varsayılan yapılandırma ayarlarını görüntüleyebilmek için

Terminal - bash

File Edit View Terminal Tabs Help

```
>>> conf
ASN1_default_codec = <ASN1Codec BER[1]>
AS_resolver = <scapy.as_resolvers.AS_resolver_multi instance at 0x7fdaca1ce128>
BTsocket   = <BluetoothL2CAPSocket: read/write packets on a connected L2CAP ...
L2listen   = <L2ListenSocket: read packets at layer 2 using Linux PF_PACKET ...
L2socket   = <L2Socket: read/write packets at layer 2 using Linux PF_PACKET ...
L3socket   = <L3PacketSocket: read/write packets at layer 3 using Linux PF_P...
auto_fragment = 1
checkIPID  = 0
checkIPaddr = 1
checkIPsrc = 1
check_TCPerror_seqack = 0
color_theme = <DefaultTheme>
commands   = arpcachepoison : Poison target's cache with (your MAC,victim's ...
debug_dissector = 0
debug_match = 0
default_l2 = <class 'scapy.packet.Raw'>
emph       = <Emphasize []>
ethertypes = </etc/ethertypes/ >
except_filter = ''
extensions_paths = '.'
histfile   = '/home/securityci/.scapy_history'
iface      = 'eth0'
iface6     = 'lo'
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Varsayılan yapılandırma ayarları üzerinde değişiklik yapabilmek için:

Terminal - bash

File Edit View Terminal Tabs Help

```
>>> conf.iface
'eth0'
>>> conf.iface = "wlan0mon"
>>>
>>> conf.iface
'wlan0mon'
>>>
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Desteklenen protokolleri görebilmek için:

```
Terminal - bash
File  Edit  View  Terminal  Tabs  Help
>>> ls()
AH          : AH
ARP         : ARP
ASN1_Packet : None
BOOTP       : BOOTP
CookedLinux : cooked linux
DHCP        : DHCP options
DHCP6       : DHCPv6 Generic Message)
DHCP6OptAuth : DHCP6 Option - Authentication
DHCP6OptBCMCSDomains : DHCP6 Option - BCMCS Domain Name List
DHCP6OptBCMCSServers : DHCP6 Option - BCMCS Addresses List
DHCP6OptClientFQDN : DHCP6 Option - Client FQDN
DHCP6OptClientId : DHCP6 Client Identifier Option
DHCP6OptDNSDomains : DHCP6 Option - Domain Search List option
DHCP6OptDNSServers : DHCP6 Option - DNS Recursive Name Server
DHCP6OptElapsedTime : DHCP6 Elapsed Time Option
DHCP6OptGeoConf :
DHCP6OptIAAddress : DHCP6 IA Address Option (IA_TA or IA_NA suboption)
DHCP6OptIAPrefix : DHCP6 Option - IA_PD Prefix option
DHCP6OptIA_NA : DHCP6 Identity Association for Non-temporary Addresses Option
DHCP6OptIA_PD : DHCP6 Option - Identity Association for Prefix Delegation
DHCP6OptIA_TA : DHCP6 Identity Association for Temporary Addresses Option
DHCP6OptIfaceId : DHCP6 Interface-Id Option
DHCP6OptInfoRefreshTime : DHCP6 Option - Information Refresh Time
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Kullanılabilir hazır fonksiyonları görebilmek için:

Terminal - bash

File Edit View Terminal Tabs Help

```
>>> lsc()
arpcachepoison      : Poison target's cache with (your MAC,victim's IP) couple
arping              : Send ARP who-has requests to determine which hosts are up
bind_layers         : Bind 2 layers on some specific fields' values
bridge_and_sniff    : Forward traffic between two interfaces and sniff packets e
xchanged
corrupt_bits        : Flip a given percentage or number of bits from a string
corrupt_bytes       : Corrupt a given percentage or number of bytes from a strin
g
defrag              : defrag(plist) -> ([not fragmented], [defragmented],
defragment          : defrag(plist) -> plist defragmented as much as possible
dyndns_add          : Send a DNS add message to a nameserver for "name" to have
a new "rdata"
dyndns_del          : Send a DNS delete message to a nameserver for "name"
etherleak           : Exploit Etherleak flaw
fragment            : Fragment a big IP datagram
fuzz                : Transform a layer into a fuzzy layer by replacing some def
ault values by random objects
getmacbyip          : Return MAC address corresponding to a given IP address
hexdiff             : Show differences between 2 binary strings
hexdump             : --
hexedit             : --
is_promisc          : Try to guess if target is in Promisc mode. The target is p
rovided by its ip.
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Bir fonksiyonun kullanımı hakkında bilgi alabilmek için:

Terminal - scapy

File Edit View Terminal Tabs Help

```
>>> help(arping)
```

Terminal - bash

File Edit View Terminal Tabs Help

```
Help on function arping in module scapy.layers.l2:

arping(net, timeout=2, cache=0, verbose=None, **kargs)
    Send ARP who-has requests to determine which hosts are up
    arping(net, [cache=0,] [iface=conf.iface,] [verbose=conf.verb]) -> None
    Set cache=True if you want arping to modify internal ARP-Cache
(END)
```

Sniff Fonksiyonu ile Analize Başlamak

Terminal - bash

File Edit View Terminal Tabs Help

```
Help on function sniff in module scapy.sendrecv:

sniff(count=0, store=1, offline=None, prn=None, lfilter=None, L2socket=None, tim
eout=None, opened_socket=None, stop_filter=None, *arg, **karg)
    Sniff packets
    sniff([count=0,] [prn=None,] [store=1,] [offline=None,] [lfilter=None,] + L2
ListenSocket args) -> list of packets

      count: number of packets to capture. 0 means infinity
      store: wether to store sniffed packets or discard them
        prn: function to apply to each packet. If something is returned,
             it is displayed. Ex:
             ex: prn = lambda x: x.summary()
    lfilter: python function applied to each packet to determine
             if further action may be done
             ex: lfilter = lambda x: x.haslayer(Padding)
    offline: pcap file to read packets from, instead of sniffing them
    timeout: stop sniffing after a given time (default: None)
    L2socket: use the provided L2socket
    opened_socket: provide an object ready to use .recv() on
    stop_filter: python function applied to each packet to determine
                 if we have to stop the capture after this packet
                 ex: stop_filter = lambda x: x.haslayer(TCP)
(END)
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

sniff(iface=‘mon0’,count=‘paketsayısı’, prn=Fonksiyon)

- **İface** = monitör moda aldığımız ve sniff işleminde kullanacağımız ağ kartı tanımlaması
- **Count** = sniff edilecek paket sayısı
- **Prn** = sniff edilen paketlerin işleme sokulacağı fonksiyon

Scapy ile Adım Adım Kablosuz Ağ Analizi

Scapy ile Sniffing İşlemine Başlamak

Kablosuz ağ sniffing işlemine başlamak için öncelikle ağ kartınızın monitör mode destekliyor olması lazım.

Bunun için aşağıdaki ağ adaptörleri tercih edilebilir.

- Atheros (AR5XXX, AR9XXX)
- Broadcom (B43XX Family)
- Intel Pro Wireless and Intel Wifi Link (Centrino)
- Ralink (RT2X00)
- Realtek (RTL8187)

Scapy ile Adım Adım Kablosuz Ağ Analizi

Ağ kartını monitör moda almak (1)

```
~ @ 20:35:03
$ sudo airmon-ng start wlan0
[sudo] password for securityci:


Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
576     avahi-daemon
577     avahi-daemon
861     NetworkManager
3096    dhclient
3721    wpa_supplicant


Interface       Chipset         Driver

wlan0           Atheros         ath9k - [phy0]
                                (monitor mode enabled on mon0)
```

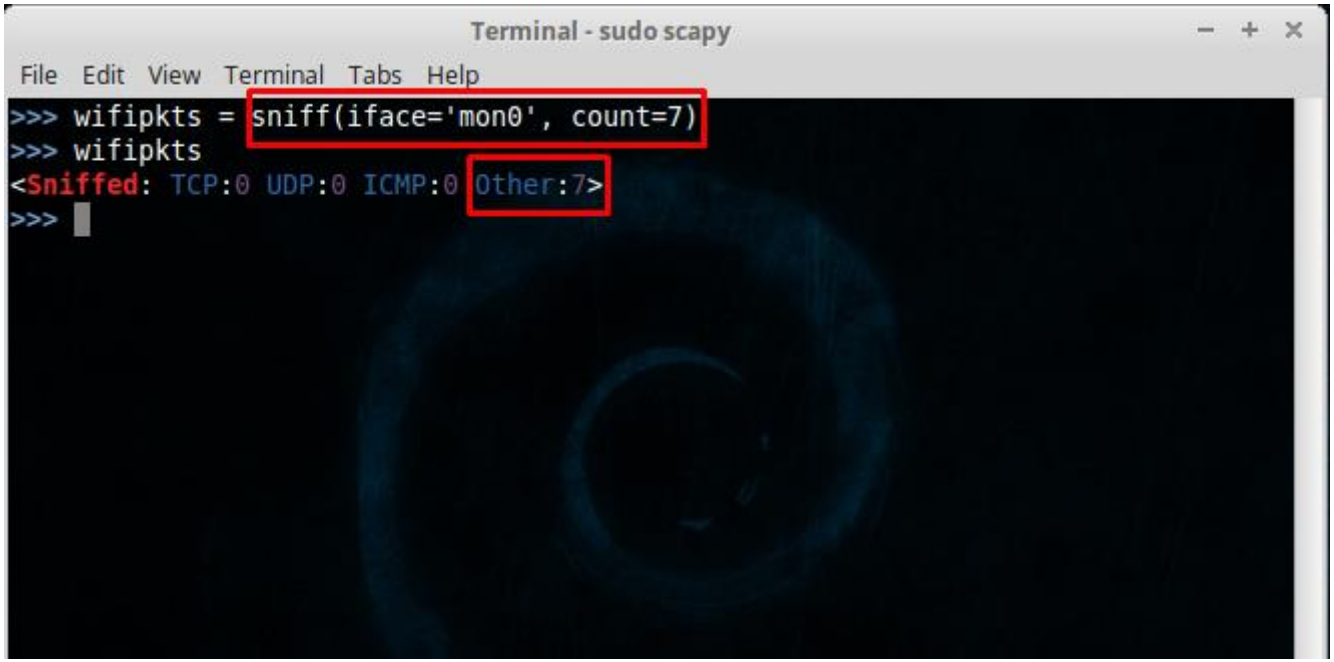
Scapy ile Adım Adım Kablosuz Ağ Analizi

Ağ kartını monitör moda almak (2)

```
Terminal - securityci@max: ~
File  Edit  View  Terminal  Tabs  Help
~ ⊙ 0:06:58
$ sudo ifconfig wlan0 down
[sudo] password for securityci:

~ ⊙ 0:07:19
$ sudo iwconfig wlan0 mode monitor

~ ⊙ 0:07:32
$ ifconfig wlan0 up
SIOCSIFFLAGS: Operation not permitted

~ ⊙ 0:07:38
$ sudo ifconfig wlan0 up

~ ⊙ 0:07:42
$ iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11bgn  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

lo        no wireless extensions.


~ ⊙ 0:07:49
$
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

İlk sniffing işlemi:



Scapy ile Adım Adım Kablosuz Ağ Analizi

Yakalanan paketlerin detaylarını görüntüleyebilmek için:

Terminal - sudo scapy

File Edit View Terminal Tabs Help

```
>>> wifipkts.nsummary()
0000 RadioTap / 802.11 Management 8L 54:e6:fc:c1:07:e8 > ff:ff:ff:ff:ff:ff / Dot
11Beacon / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot11El
t / Dot11Elt / Dot11Elt / Dot11Elt
0001 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
0002 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
0003 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
0004 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
0005 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
0006 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
>>>
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Paketlerden sadece birini incelemek için:

Terminal - sudo scapy

File Edit View Terminal Tabs Help

```
>>> pkt0 = wifipkts[0]
>>> pkt0
<RadioTap  version=0 pad=0 len=36 present=TSFT+Flags+Rate+Channel+dBm_AntSignal+
b14+b29+Ext notdecoded=' \x08\x00\x00\x00\x00\x00\x00\xe6\xeb\xae?\x00\x00\x01\x
00\x10\x02l\t\xa0\x00\xa4\x00\x00\x00\xa4\x00' |<Dot11  subtype=8L type=Manageme
nt proto=0L FCfield= ID=0 addr1=ff:ff:ff:ff:ff:ff addr2=54:e6:fc:c1:07:e8 addr3=
54:e6:fc:c1:07:e8 SC=20672 addr4=None |<Dot11Beacon  timestamp=1225215693185 bea
con_interval=100 cap=short-slot+ESS+privacy+short-preamble |<Dot11Elt  ID=SSID l
en=8 info='dejavu-2' |<Dot11Elt  ID=Rates len=8 info='\x82\x84\x8b\x96\x0c\x180H
' |<Dot11Elt  ID=DSset len=1 info='\x01' |<Dot11Elt  ID=TIM len=42 info='\x00\x0
1\x00\x06\x00\x00\x00\x00\x10\x00\x02\x00B\x01P\x02\x00\x10\x00\x00\x02\x00\x84\
x00\x00\x83\x00@\x00\x02\x00\x00\x00\x00\x02E\x00\x02\x00\x00\x04\x10' |<Dot11El
t  ID=ERPinfo len=1 info='\x00' |<Dot11Elt  ID=ESRates len=4 info='\x12$`l' |<Do
t11Elt  ID=RSNinfo len=24 info='\x01\x00\x00\x0f\xac\x02\x02\x00\x00\x0f\xac\x02
\x00\x0f\xac\x04\x01\x00\x00\x0f\xac\x02\x01\x00' |<Dot11Elt  ID=vendor len=26 i
nfo='\x00P\xf2\x01\x01\x00\x00P\xf2\x02\x02\x00\x00P\xf2\x02\x00P\xf2\x04\x01\x0
0\x00P\xf2\x02' |<Dot11Elt  ID=99 len=72 info='\x92\x10' |>>>>>>>>>>>>>
>>>
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Bir Paketin Anatomisi

- **Radiotap Header kısmında:**

Kanal numarası ve dbm cinsinden sinyal gücü gibi değerler yer almaktadır

No.	Time	Source	Destination	Protocol	Length
1	0.000000	Tp-LinkT_c1:07:e8	Broadcast	802.11	206

```
▸ Frame 1: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits)
▾ Radiotap Header v0, Length 36
    Header revision: 0
    Header pad: 0
    Header length: 36
  ▸ Present flags
    MAC timestamp: 281476045138918
  ▸ Flags: 0x10
    Data Rate: 1,0 Mb/s
    Channel frequency: 2412 [BG 1]
  ▸ Channel type: 802.11b (0x00a0)
    SSI Signal: -92 dBm
  ▸ RX flags: 0x0000
    SSI Signal: -92 dBm
    Antenna: 0
▸ IEEE 802.11 Beacon frame, Flags: ........C
▸ IEEE 802.11 wireless LAN management frame
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Bir Paketin Anatomisi

- **Dot11 Katmanı:**

```
▾ IEEE 802.11 wireless LAN management frame
  ▾ Fixed parameters (12 bytes)
      Timestamp: 0x0000011d448bd181
      Beacon Interval: 0,102400 [Seconds]
    ▾ Capabilities Information: 0x0431
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator
        .... .... ...1 .... = Privacy: AP/STA can support WEP
        .... .... ..1. .... = Short Preamble: Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
  ▸ Tagged parameters (130 bytes)
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Bir Paketin Anatomisi

- **Dot11Elt Katmanı:**

```
▶ Radiotap Header v0, Length 36
▶ IEEE 802.11 Beacon frame, Flags: ........C
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (130 bytes)
    ▶ Tag: SSID parameter set: dejavu-2
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 12, 24, 36, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 1
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: ERP Information
    ▶ Tag: Extended Supported Rates 9, 18, 48, 54, [Mbit/sec]
    ▶ Tag: RSN Information
    ▶ Tag: Vendor Specific: Microsof: WPA Information Element
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Bir Paketin Anatomisi

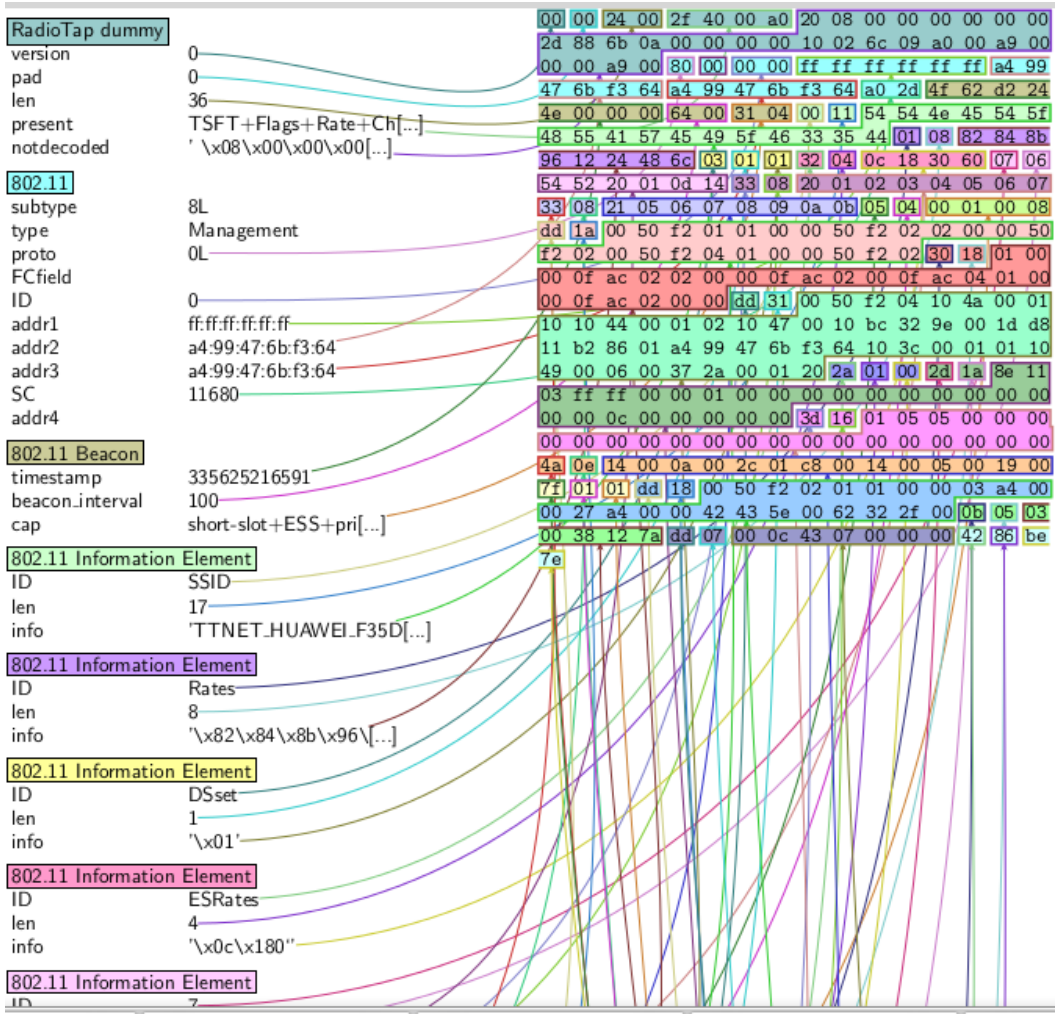
- **İncelenen paketin katmanlarındaki değerlere erişmek:**

```
File  Edit  View  Terminal  Tabs  Help
>>> pkt0
<RadioTap  version=0 pad=0 len=36 present=TSFT+Flags+Rate+Channel+dBm_AntSignal+
b14+b29+Ext notdecoded=' \x08\x00\x00\x00\x00\x00\x00\xe6\xeb\xae?\x00\x00\x01\x
00\x10\x02l\t\xa0\x00\xa4\x00\x00\x00\xa4\x00' |<Dot11  subtype=8L type=Manageme
nt proto=0L FCfield= ID=0 addr1=ff:ff:ff:ff:ff:ff addr2=54:e6:fc:c1:07:e8 addr3=
54:e6:fc:c1:07:e8 SC=20672 addr4=None |<Dot11Beacon  timestamp=1225215693185 bea
con_interval=100 cap=short-slot+ESS+privacy+short-preamble |<Dot11Elt  ID=SSID l
en=8 info='dejavu-2' |<Dot11Elt  ID=Rates len=8 info='\x82\x84\x8b\x96\x0c\x18\x30
' |<Dot11Elt  ID=DSset len=1 info='\x01' |<Dot11Elt  ID=TIM len=42 info='\x00\x0
1\x00\x06\x00\x00\x00\x00\x10\x00\x02\x00B\x01P\x02\x00\x10\x00\x00\x02\x00\x84\
x00\x00\x83\x00@\x00\x02\x00\x00\x00\x00\x02E\x00\x02\x00\x00\x04\x10' |<Dot11El
t  ID=ERPinfo len=1 info='\x00' |<Dot11Elt  ID=ESRates len=4 info='\x12$`l' |<Do
t11Elt  ID=RSNinfo len=24 info='\x01\x00\x00\x0f\xac\x02\x02\x00\x00\x0f\xac\x02
\x00\x0f\xac\x04\x01\x00\x00\x0f\xac\x02\x01\x00' |<Dot11Elt  ID=vendor len=26 i
nfo='\x00P\xf2\x01\x01\x00\x00P\xf2\x02\x02\x00\x00P\xf2\x02\x00P\xf2\x04\x01\x0
0\x00P\xf2\x02' |<Dot11Elt  ID=99 len=72 info='\x92\x10' |>>>>>>>>>>>>>
>>> pkt0[Dot11Elt].info
'dejavu-2'
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Bir Paketin Anatomisi

- **İncelenen paketin pdfdump() ile analizi:**



Scapy ile Adım Adım Kablosuz Ağ Analizi

Yakaladığımız paketleri pcap formatında kayıt etmek için:

Terminal - sudo scapy

File Edit View Terminal Tabs Help

```
>>> wrpcap("scapy_e.pcap", wifipkts)
>>>
```

Terminal - securityci@max: ~

File Edit View Terminal Tabs Help

```
~ ⊙ 21:47:40
$ ls
capture-2.avi  Documents  out.ogv       Templates  work
capture-2.wmv  Downloads  Pictures      Videos     www.besimaltinok.com
ddd            Music      Public        wget.log
Desktop        out-1.ogv  scapy_e.pcap  wget_work

~ ⊙ 21:47:41
$
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

pcap formatındaki bir dosyayı okumak için:

Terminal - sudo scapy

File Edit View Terminal Tabs Help

```
>>> wifipkts1 = rdpcap("scapy_e.pcap")
>>> wifipkts1
<scapy_e.pcap: TCP:0 UDP:0 ICMP:0 Other:7>
>>> wifipkts1.nsummary()
0000 RadioTap / 802.11 Management 8L 54:e6:fc:c1:07:e8 > ff:ff:ff:ff:ff:ff / Dot
11Beacon / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot11El
t / Dot11Elt / Dot11Elt / Dot11Elt
0001 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
0002 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
0003 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
0004 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
1Elt / Dot11Elt / Dot11Elt
0005 RadioTap / 802.11 Management 5L 54:e6:fc:c1:07:e8 > 54:e6:fc:c1:06:8c / Dot
11ProbeResp / SSID='dejavu-2' / Dot11Elt / Dot11Elt / Dot11Elt / Dot11Elt / Dot1
```

Scapy ile Adım Adım Kablosuz Ağ Analizi

Paket Analizinde işimize yarayacak Notlar

ord(pkt0[Dot11Elt:3].info)	== Kanal numarası bilgisini verir.
256-(ord(pkt.notdecoded[-4:-3]))	== Sinyal gücü
pkt0.type	== 0 [Managment Frame]
pkt0.subtype	== 8 [Beacon Frame]
pkt0.addr2	== AP cihazının adresi
pkt0.info	== SSID bilgisi

Scapy ile Alıştırmalar

OPN Ağları Bulmak

```
from scapy.all import *

open_networks = []
ap_list       = []


def PacketHandlers(pkt) :

   if pkt.haslayer(Dot11) :
      if pkt.type == 0 and pkt.subtype == 8 :
         if pkt.addr2 not in ap_list :
            ap_list.append(pkt.addr2)
               open_ssid  = pkt.info
               open_bssid = pkt.addr2
               cap = pkt.sprintf("{Dot11Beacon:%Dot11Beacon.cap%}"
                                 "{Dot11ProbeResp:%Dot11ProbeResp.cap%}").split('+')

               if 'privacy' not in cap and pkt.info != '':
                  print "Detect Open Network MAC Addres : %s and SSID : %s " %(open_bssid, open_ssid)



sniff(iface='wlan0mon', count=999999, prn=PacketHandlers)
```

Scapy ile Alıştırmalar

Gizli SSID Bilgilerini Toplamak

```
__author__ = 'besimaltnok'

from scapy.all import *

hidden_ssid = []
find_ssid   = []

def FindHiddenSSID(pkt):
        if pkt.type == 0 and pkt.subtype == 8 :
                if not pkt.info:
                        if pkt.addr2 not in hidden_ssid:
                                hidden_ssid.append(pkt.addr2)

        elif pkt.haslayer(Dot11ProbeResp) and pkt.addr2 in hidden_ssid:
            if pkt.addr2 not in find_ssid:
              find_ssid.appen(pkt.addr2)
                          print pkt.addr2, pkt.info

sniff(iface='wlan0mon',count=9999999,prn=FindHiddenSSID)
```

Scapy ile Alıştırmalar

Deauthentication Attacks Monitör

```
#!/usr/bin/env python

__author__ = 'besimaltnok'

import os
from scapy.all import sniff

deattack    = []

imon = 'mon0'

def FindDeauth(pkt):
    if pkt.type == 0 and pkt.subtype == 12:
        client = (pkt.addr1).upper()
        AP     = (pkt.addr2).upper()
        if client not in deattack:
            deattack.append(client)
            info = "De-Attack to : " + AP + "on AP : ", client
            print info

sniff(iface=imon , count=23232, prn=FindDeauth)
```