

# Kablosuz Ağlar ve Güvenlik

**Huzeyfe ÖNAL**  
**huzeyfe@enderunix.org**

# Sunum Planı

- Kablosuz Ağlar
- Kablosuz Ağ Protokolleri
- Temel WLAN Güvenliği
- Güvenlik Riskleri
- Güvenlik(?) Amaçlı Kullanılan Yazılımlar
- Güvenli Kablosuz ağ kullanımı için tavsiyeler

# Neden Kablosuz Ağ?

- Kablo derdine son!
- Göreceli olarak TOC daha düşük.
- Gezgin ofis kullanıcıları için ideal
- Son kullanıcıda ağ ayarı gerektirmiyor
- El terminalleri ile iş imkanı..
- Fiziksel Güvenlik yok (-)
- Düşük bant genişliği (-)

# Kablosuz Ağ Kavramları

- Frame
- Access point
- IEEE 802.11
- SSID
- WEP
- WPA (Wi-Fi Protected Access)





# Yaygın kablosuz ağ yöntemleri

- Ad-hoc
  - Independent Basic service set olarak da bilinir (IBSS)
  - AP'ye gerek duymadan wireless cihazların bir biri arasında haberleşmesi
- Infrastructure mode
  - Basic Service Set olarak bilinir. (BSS)
  - En azından bir AP (Access Point) ve Wireless cihaz gerektirir
  - Haberleşme SSID ve her iki tarafa girilen bir key aracılığı ile olur
  - İstemci direk karşı taraf ile konuştuğunu zanneder fakat bütün trafik AP üzerinden geçer.

# Linux wlan komutlari

```
root@slax:~# iwconfig rausb0
rausb0    RT2500USB WLAN  ESSID:"misafir"
          Mode:Managed  Frequency:2.432GHz  Access Point: 00:13:21:57:F8:FD
          Bit Rate=11Mb/s
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Link Quality:61/100  Signal level:-75 dBm  Noise level:-200 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

root@slax:~# iwconfig rausb0 essid misafir
root@slax:~# iwconfig rausb0
rausb0    RT2500USB WLAN  ESSID:"misafir"
          Mode:Managed  Frequency:2.432GHz  Access Point: 00:13:21:57:F8:FD
          Bit Rate=11Mb/s
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Link Quality:58/100  Signal level:-74 dBm  Noise level:-200 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

root@slax:~# █
```

# Linux'u AP olarak kullanmak

- Ad-hoc mode için
- ifconfig eth0 mode hostap essid "Sebil"
- HOSTAP yazılımı
  - Sahte beacon paketleri
  - WLAN dos saldırısı



# Kablosuz Ağ Protokolleri-I

- 802.11b
  - 2.4 Ghz band aralığında çalışır
  - Max bant genişliği 11Mbps
  - 3\*-75m arası performans
  - Günümüzde yaygın kullanılıyor
- 802.11a
  - 5GHz band aralığında yayın yapar
  - Max band genişliği 54Mbps
  - 25-50m civarında performans



# Kablosuz Ağ Protokolleri-II

- 802.11g
  - 802.11b uyumlu
  - 2.4 GHz aralığında
  - 54 Mbps'e kadar çıkan hız
- 802.11i
  - WLAN güvenliği için düşünülmüş
  - 802.11a ve 802.11b WLAN'lari arasındaki iletişimin şifrelenmesini belirler
  - AES TKIP(temporary key integrity protocol) gibi yeni şifreleme metodları kullanır

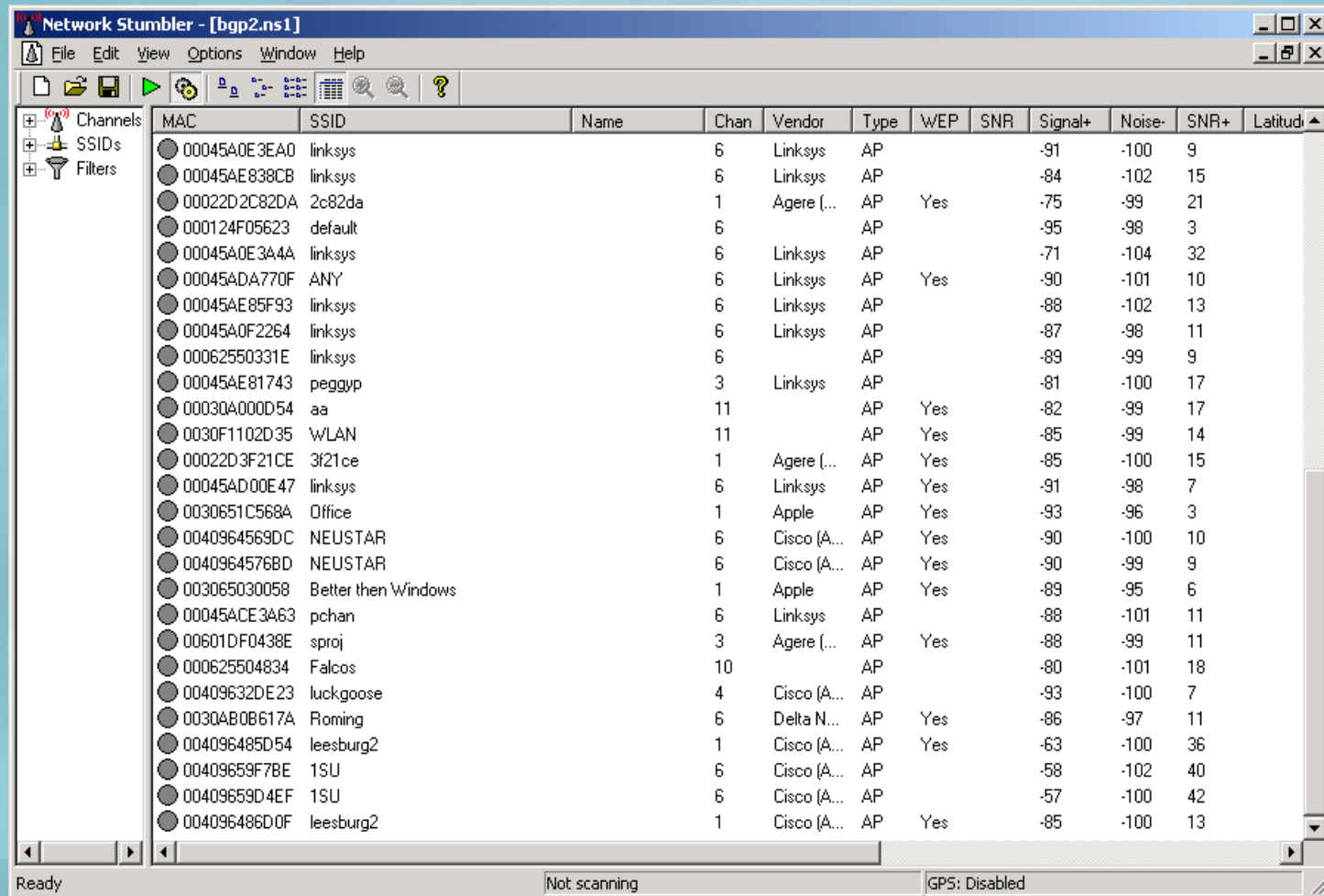
# 802.11 Standartları..



# Temel Güvenlik

- SSID
  - AP'nin adı denilebilir.
  - SSID ne kadar karışık seçerseniz seçin görünecektir,
  - Saklasanız bile.
  - WEP kullanımı bunu engellemez(SSID Anonsları şifrelenmez)
  - Araç: Network Stumbler, Kismet

# Network Stumbler..



Network Stumbler - [bpg2.ns1]

File Edit View Options Window Help

Channels SSIDs Filters

MAC	SSID	Name	Chan	Vendor	Type	WEP	SNR	Signal+	Noise-	SNR+	Latitud
00045A0E3EA0	linksys		6	Linksys	AP			-91	-100	9	
00045AE838CB	linksys		6	Linksys	AP			-84	-102	15	
00022D2C82DA	2c82da		1	Agere (...)	AP	Yes		-75	-99	21	
000124F05623	default		6		AP			-95	-98	3	
00045A0E3A4A	linksys		6	Linksys	AP			-71	-104	32	
00045ADA770F	ANY		6	Linksys	AP	Yes		-90	-101	10	
00045AE85F93	linksys		6	Linksys	AP			-88	-102	13	
00045A0F2264	linksys		6	Linksys	AP			-87	-98	11	
00062550331E	linksys		6		AP			-89	-99	9	
00045AE81743	peggyp		3	Linksys	AP			-81	-100	17	
00030A000D54	aa		11		AP	Yes		-82	-99	17	
0030F1102D35	WLAN		11		AP	Yes		-85	-99	14	
00022D3F21CE	3f21ce		1	Agere (...)	AP	Yes		-85	-100	15	
00045AD00E47	linksys		6	Linksys	AP	Yes		-91	-98	7	
0030651C568A	Office		1	Apple	AP	Yes		-93	-96	3	
0040964569DC	NEUSTAR		6	Cisco (A...	AP	Yes		-90	-100	10	
0040964576BD	NEUSTAR		6	Cisco (A...	AP	Yes		-90	-99	9	
003065030058	Better then Windows		1	Apple	AP	Yes		-89	-95	6	
00045ACE3A63	pchan		6	Linksys	AP			-88	-101	11	
00601DF0438E	sproj		3	Agere (...)	AP	Yes		-88	-99	11	
000625504834	Falcos		10		AP			-80	-101	18	
00409632DE23	luckgoose		4	Cisco (A...	AP			-93	-100	7	
0030AB0B617A	Roming		6	Delta N...	AP	Yes		-86	-97	11	
004096485D54	leesburg2		1	Cisco (A...	AP	Yes		-63	-100	36	
00409659F7BE	1SU		6	Cisco (A...	AP			-58	-102	40	
00409659D4EF	1SU		6	Cisco (A...	AP			-57	-100	42	
004096486D0F	leesburg2		1	Cisco (A...	AP	Yes		-85	-100	13	

Ready Not scanning GPS: Disabled



# Erişim/Onaylama Kontrolü

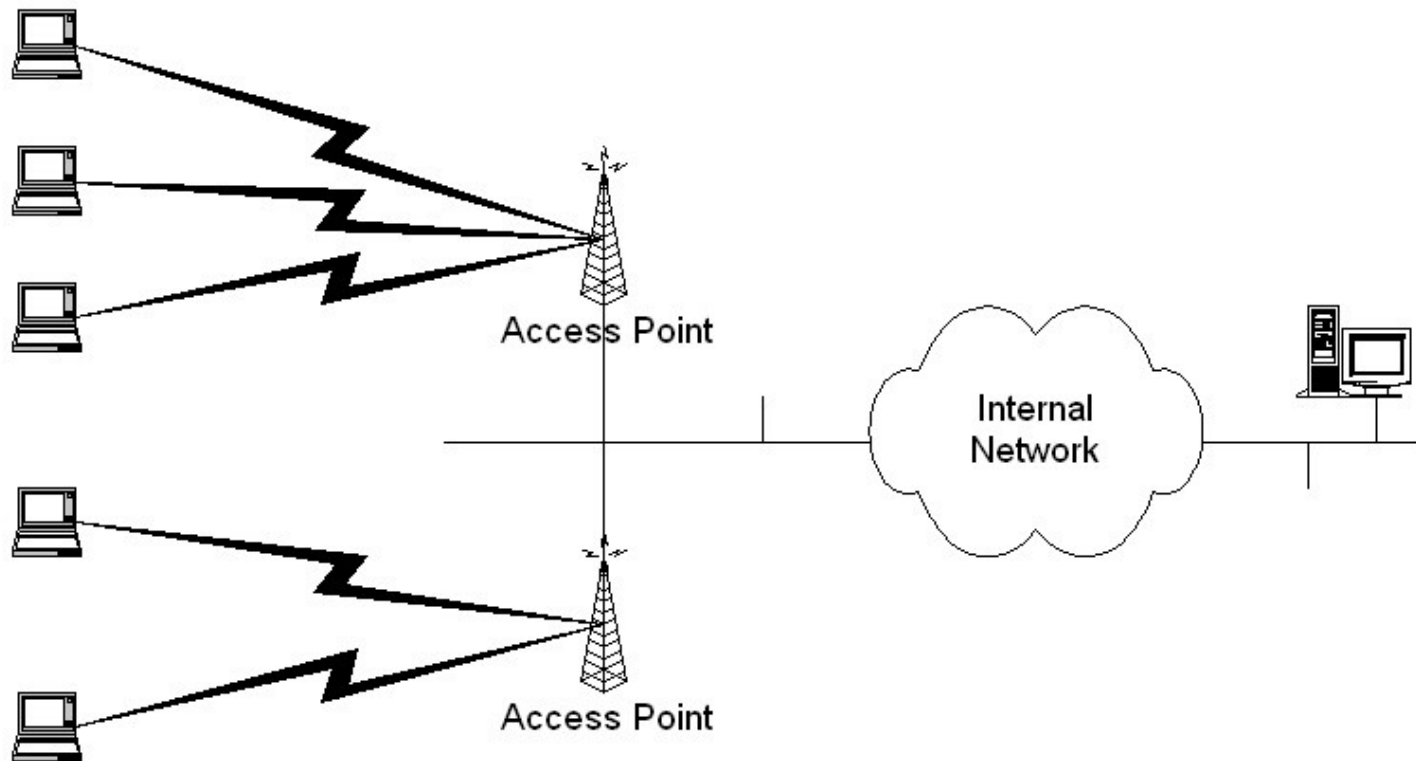
- Hangi kullanıcılar WLAN kullanma hakkına sahip?
  - Anahtarı bilen her kullanıcı ağa girebilir
  - Her kullanıcıya ait bir hesap olmalı(en azından)
- MAC tabanlı erişim kontrolü
  - AP ile İstemci arasındaki MAC adresleri açık bir şekilde gider
  - MAC adreslerini değiştirmek oldukça kolay

# Kullanıcı Onaylama..

Supplicant

Authenticator

Authentication  
Server

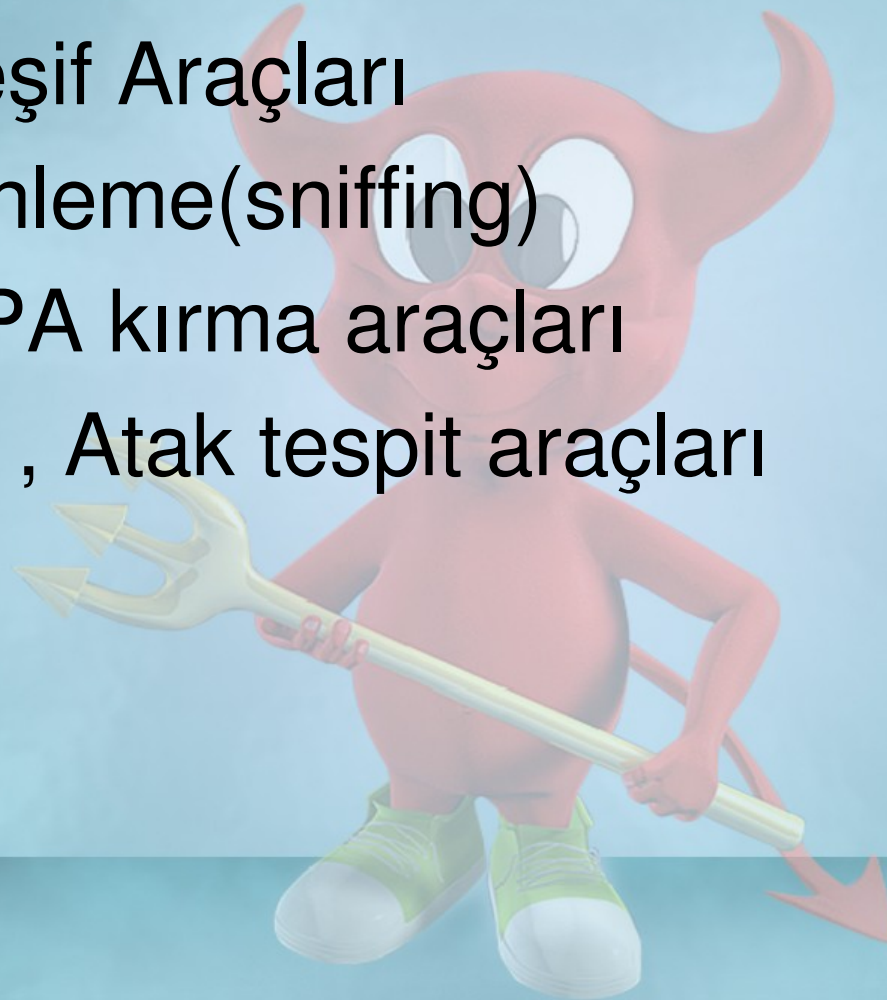


# WEP(Wired Equivalent Privacy)

- Sadece veri transferini şifreler..
- Her iki tarafın bildiği paylaşımlı bir anahtarın kullanılır (RC4)
- Kimlik doğrulama yok!
- Kompleksliğine bağlı olarak rahatlıkla kırılabilir(40-64/104-128 bit)
  - Belirli miktar trafik kaydedilmeli.
- Ten minutes Wep crack!

# Kullanılan Araçlar

- WLAN keşif Araçları
- WLAN dinleme(sniffing)
- WEP, WPA kırma araçları
- Korunma , Atak tespit araçları
- weplabs





# Kablosuz ağlarda keşif?

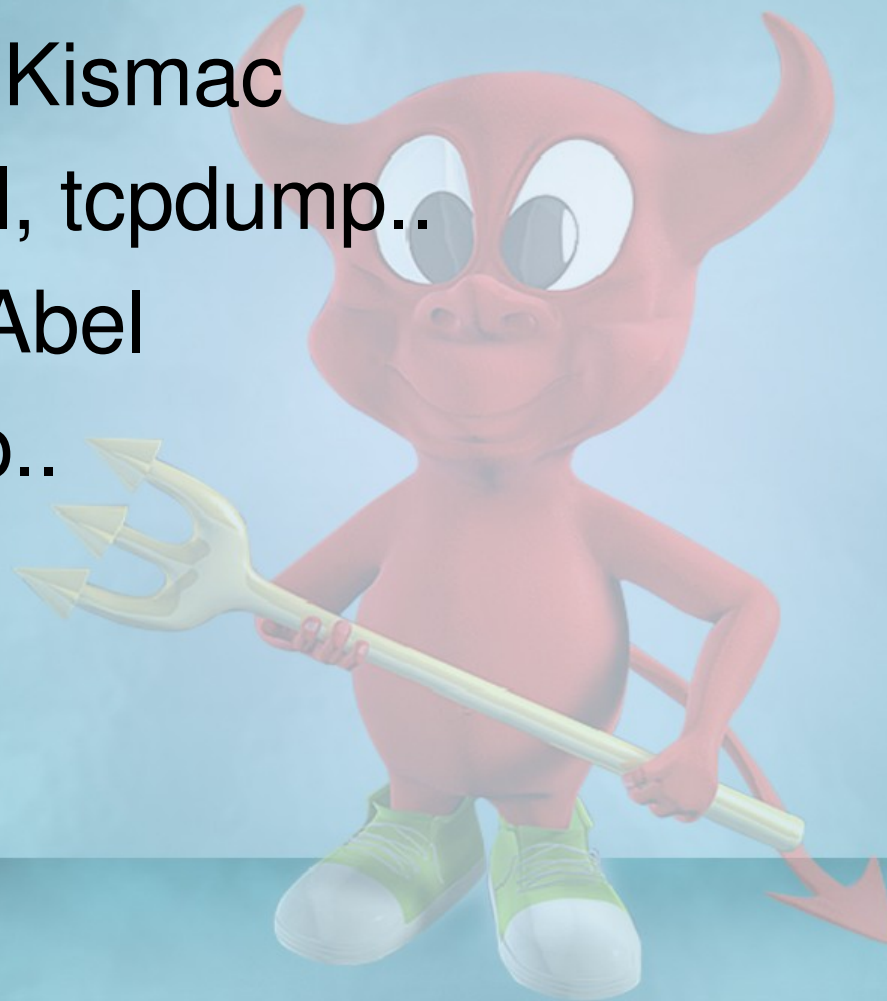
- Çalışan AP'leri bulma yöntemi
  - Pasif ve Aktif Keşif
  - Kismet ile pasif keşif..
- WAR Driving
  - NetStumbler, BSD-AirTools , AirSnort
- WarChalking
  - yol kenarlarına vs orada bir kablosuz ağın olduğunu belirten işaretler yapmak.

# WAR Driving..



# Dinleme Araçları

- Kismet, Kismac
- Ethereal, tcpdump..
- Cain & Abel
- Ettercap..





# Kismet- Wireless Sniffer

ipw-Apr-30-2006-1.dump

lilo.conf

ipw-Apr-30-2006-1.gps

ipw-Apr-30-2006-1.net...

ipw-Apr-30-2006-1.csv

ipw-Apr-30-2006-1.xml

### Kismet eth1

Network List (Autofit)

Name	Client	Type	Channel	Rate	SignalGraph	Noise	Packets	Flags	IP Range	Size	DIV	Weak
wave	1 A N	006	22.0			0	17		0.0.0.0	124B	0	0
misafir	44 A N	001	0.0			-25	447	02	144.122.0.0	25k	0	0
misafir	9 A N	005	36.0			0	113	T3	144.122.5.0	1k	0	0
misafir	30 A N	009	36.0			-25	945	04	144.122.5.183	24k	0	0
misafir	22 A N	001	36.0			-25	185	02	144.122.0.0	8k	0	0
misafir	21 A N	005	36.0			-25	321	04	144.122.5.183	8k	0	0
misafir	1 A N	005	36.0			0	4	04	10.62.33.252	106B	0	0
misafir	0 A N	001	36.0			0	1	T4	144.122.4.12	0B	0	0
Gro ssid	0 A N	007	34.0			0	4		0.0.0.0	0B	0	0
Data Networks	9 C N	005	0.0			0	60	G	0.0.0.0	2k	0	0

Info

Ntorks: 11

Packets: 2123

Cryptd: 5

Weak: 0

Noise: 6

Discrd: 5

Pkts/s: 32

Hostap: Ch: 8

Elapsed: 00:02:21

Status

Found IP 144.122.5.92 for misafir:00:12:F0:61:91:B9 via TCP

Found IP 144.122.5.171 for misafir:00:12:F0:31:20:FD via ARP

Found IP 144.122.4.23 for misafir:00:13:CE:27:2A:21 via TCP

Found IP 144.122.5.92 for misafir:00:12:F0:61:91:B9 via UDP

Battery: unavailable

Kismet eth1

2

12:25



# Kismet – AP Kesfi

Network List (SSID)

Info

Network Details

Name : misafir

+

SSID : misafir

Server : localhost:2501

BSSID : 00:13:21:57:F8:FD

Manuf : Unknown

Max Rate: 36.0

BSS Time: 4b7f7f1181

First : Sun May 14 12:23:22 2006

Latest : Sun May 14 12:27:13 2006

Clients : 30

Type : Access Point (infrastructure)

Info :

Channel : 5

Privacy : No

Encrypt : None

Beacon : 25600 (26,214400 sec)

Packets : 678

Data : 97

LLC : 580

Crypt : 1

Weak : 0

Dupe IV : 0

Data : 13k (14187B)

Signal :

Power : -256 (best -256)

Noise : -256 (best -256)

IP Type : DHCP

IP Range: 144.122.5.183

Min Loc : N/A

Max Loc : N/A

Range : N/A

Found IP 169.254.250.97 for misafir::00:0E:35:EE:4F:5F via TCP

Battery: unavailable

# IP araligini Bulma

Network List (SSID)							Info	
Client List (Autofit)								
T	MAC	Manuf	Data	Crypt	Size	IP Range	Sgn	Nse
+	F 00:0E:38:A8:D4:05	Cisco	61	0	4k	0.0.0.0	0	0
	F 00:13:CE:18:E2:C2	Unknown	4	0	454B	10.62.33.252	0	0
	F 00:14:C1:01:20:AD	Unknown	1	0	128B	144.122.4.49	0	0
	F 00:16:6F:02:CC:61	Unknown	3	0	728B	144.122.4.162	0	0
	F 00:13:CE:98:8E:36	Unknown	4	0	440B	10.62.32.240	0	0
	F 00:12:F0:66:7D:3E	IntelCor	11	0	1k	169.254.12.104	0	0
	F 00:12:F0:80:17:46	IntelCor	19	0	1k	144.122.5.197	0	0
	F 00:13:CE:5F:E5:D7	Unknown	3	0	454B	144.122.5.82	0	0
	F 00:13:CE:27:2A:21	Unknown	25	0	3k	144.122.4.23	0	0
	F 00:15:00:35:00:3B	Unknown	20	0	3k	144.122.4.216	0	0
	F 00:11:09:9B:6A:58	Micro-St	12	0	2k	216.86.145.3	0	0
	F 00:0E:35:0F:A9:A4	Intel	5	0	540B	144.122.4.41	0	0
	F 00:0D:F0:1C:45:C3	Unknown	0	0	0B	0.0.0.0	0	0
	F 00:13:49:10:00:94	Unknown	8	0	1k	144.122.4.130	0	0
	F 00:15:00:4D:39:F3	Unknown	0	0	0B	0.0.0.0	0	0
	E 00:01:24:F0:AA:B0	SMC	5	0	510B	10.62.32.252	0	0
	F 00:14:A4:3C:D3:63	Unknown	8	0	1k	144.122.4.200	0	0
	F 00:15:00:23:47:95	Unknown	12	0	1k	144.122.4.135	0	0
	F 00:0C:F1:0C:30:90	Intel	0	0	0B	0.0.0.0	0	0
	F 00:01:F4:25:04:14	Unknown	2	0	222B	0.0.0.0	0	0
	F 00:12:F0:02:7A:65	IntelCor	2	0	220B	144.122.5.74	0	0
	F 00:12:F0:65:14:31	IntelCor	0	0	0B	0.0.0.0	0	0
	F 00:13:CE:6D:0B:65	Unknown	2	0	224B	10.62.33.249	0	0
	F 00:0E:83:F1:31:42	Cisco	17	0	2k	144.122.5.183	0	0
	F 00:12:BF:67:32:D8	Unknown	10	0	1k	144.122.5.131	0	0
	F 00:13:CE:0A:9A:31	Unknown	7	0	1k	144.122.4.245	0	0
	F 00:13:CE:DD:04:94	Unknown	16	1	1k	144.122.5.78	0	0
	F 00:15:C6:24:4F:B3	Unknown	0	0	0B	0.0.0.0	0	0
	F 00:12:F0:61:91:B9	IntelCor	14	0	1k	144.122.5.92	0	0
	F 00:12:F0:31:20:FD	IntelCor	1	0	78B	144.122.5.171	0	0
	F 00:C0:49:F8:F6:5F	Unknown	3	0	234B	144.122.4.170	0	0
	F 00:0E:35:3E:BE:6E	Intel	4	0	532B	144.122.5.109	0	0
	F 00:12:F0:A3:9D:80	IntelCor	7	0	1k	144.122.4.202	0	0
	F 00:08:A1:8D:89:41	CnetTech	4	0	462B	144.122.4.52	0	0
	F 00:14:A5:4E:E8:87	Unknown	2	0	344B	144.122.5.188	0	0
	F 00:90:4B:EF:A1:02	Unknown	0	0	0B	0.0.0.0	0	0
	F 00:80:AD:08:74:A5	Unknown	8	0	1k	144.122.4.159	0	0
	F 00:01:F4:25:01:14	Unknown	1	0	111B	0.0.0.0	0	0
ALERT: Suspicious client 00:13:CE:0B:CF:6B - probing networks but never participating.								
Battery: unavailable								

# Ham Veri Analizi

```
Network List (SSID)
Data Strings Dump
MAILSLOT\BROWSE
LAPTOP
Kivanc
service:printer
default
service:printer
default
FFEHFFCCACACACACACACACACACAA
EFGCNEBKGEJCACACACACACACACABN
MAILSLOT\BROWSE
EFGCNEBKGEJCACACACACACACACABL
FFEHFFCCACACACACACACACACACAA
FFEHFFCCACACACACACACACACACAA
EFGCNEBKGEJCACACACACACACACABN
MAILSLOT\BROWSE
EFGCNEBKGEJCACACACACACACACABL
FFEHFFCCACACACACACACACACACAA
service:printer
default
service:printer
default
EBECFCBFDICACACACACACACACACA
EFGCNEBKGEJCACACACACACACACABN
MAILSLOT\BROWSE
ABRAS
EFGCNEBKGEJCACACACACACACACABL
FFEHFFCCACACACACACACACACACAA
EBECFCBFDICACACACACACACACACA
EFGCNEBKGEJCACACACACACACACABN
MAILSLOT\BROWSE
ABRAS
EFGCNEBKGEJCACACACACACACACABL
FFEHFFCCACACACACACACACACACAA
FFEHFFCCACACACACACACACACACAA
EFGCNEBKGEJCACACACACACACACABL
FFEHFFCCACACACACACACACACACAA
sevim<
MSFT 5.07
sevim<
MSFT 5.07
FFEHFFCCACACACACACACACACACAA
FFEHFFCCACACACACACACACACACAA
FFEHFFCCACACACACACACACACACAA
FFEHFFCCACACACACACACACACACAA
ALERT: Suspicious client 00:13:CE:0B:CF:6B - probing networks but never participating.
Battery: unavailable
```



# Veri Analizi-II

```
Network List (SSID)
Data Strings Dump
Host:239.255.255.250:1900
+ ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1
  Man:"ssdp:discover"
  M-SEARCH * HTTP/1.1
  Host:239.255.255.250:1900
  ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1
  Man:"ssdp:discover"
  service:printer
  default
  M-SEARCH * HTTP/1.1
  Host:239.255.255.250:1900
  ST:upnp:rootdevice
  Man:"ssdp:discover"
  service:printer
  default
  FJEPFFFCNDCCBDCCEGEEEBDBDEEGEGCA
  FHEPFCLEHFCEPFFACACACACACABO
  \MAILSLOT\BROWSE
  YOUR-212FDA14FF
  FJEPFFFCNDCCBDCCEGEEEBDBDEEGEGCA
  FHEPFCLEHFCEPFFACACACACACABO
  \MAILSLOT\BROWSE
  YOUR-212FDA14FF
  service:printer
  default
  M-SEARCH * HTTP/1.1
  Host:239.255.255.250:1900
  ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1
  Man:"ssdp:discover"
  PC13B5803Q
  PC13B5803.cevreorman.gov.tr<
  MSFT 5.07
  M-SEARCH * HTTP/1.1
  Host:239.255.255.250:1900
  ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1
  Man:"ssdp:discover"
  PC13B5803Q
  PC13B5803.cevreorman.gov.tr<
  MSFT 5.07
  MM-CA026187F3F1Q
  MM-CA026187F3F1.<
  MSFT 5.07
  MM-CA026187F3F1Q
  MM-CA026187F3F1.<

ALERT: Suspicious client 00:13:CE:0B:CF:6B - probing networks but never participating.
Battery: unavailable
```



# Ethereal - Veri Analizi

File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq 10.62.32.254 and ip.addr eq 207.46.3.9) + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
12420	479.212017	10.62.32.254	207.46.3.9	HTTP	1.1 200 OK
12593	485.965405	10.62.32.254	207.46.3.9	HTTP	1.1 200 OK
12894	495.993593	10.62.32.254	207.46.3.9	HTTP	1.1 200 OK
12902	496.216815	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK
12903	496.217800	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK
12904	496.353772	10.62.32.254	207.46.3.9	HTTP	1.1 200 OK
12908	496.571962	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK
13061	501.371309	10.62.32.254	207.46.3.9	HTTP	1.1 200 OK
13092	502.387283	10.62.32.254	207.46.3.9	HTTP	1.1 200 OK
13100	502.605784	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK
13107	503.506826	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK
13111	503.687016	10.62.32.254	207.46.3.9	HTTP	1.1 200 OK
13239	508.464206	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK
13248	508.719421	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK
13522	519.983296	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK
13739	528.894729	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK
13743	529.064944	10.62.32.254	207.46.3.9	HTTP	1.1 200 OK
13838	534.184850	207.46.3.9	10.62.32.254	HTTP	1.1 200 OK

Follow TCP stream

Stream Content:

HTTP/1.1 200 OK  
Date: Sat, 13 May 2006 09:53:51 GMT  
Server: Microsoft-IIS/6.0  
P3P:CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"  
X-Powered-By: ASP.NET  
X-MSN-Messenger: SessionID=1076698186.23257; GW-IP=207.46.3.9  
Content-Length: 159  
Content-type: application/x-msn-messenger

POST /gateway/gateway.dll?Action=poll&SessionID=1076698186.29319 HTTP/1.1  
Accept: \*/\*  
Content-Length: 0  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Windows Live Messenger/6.0.2.0)

POST /gateway/gateway.dll?Action=poll&SessionID=1076698186.17128 HTTP/1.1  
Accept: \*/\*  
Content-Length: 0  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Windows Live Messenger/6.0.2.0)

Save As Print Entire conversation (1192 bytes) Filter out this stream Close

Frame 12904 (970 bytes on wire) (IEEE 802.11)  
Type/Subtype: Data (32)  
Frame Control: 0x0108 (Normal)  
Duration: 117  
BSS Id: HewlettP\_57:e8:f9:00  
Source address: Intel\_0c:30:26:94:5a:00  
Destination address: Micro-S  
Fragment number: 0  
Sequence number: 2104

Logical-Link Control  
Internet Protocol, Src: 10.62.32.254 (10.62.32.254), Dst: 207.46.3.9 (207.46.3.9)  
Transmission Control Protocol, Src Port: nim (1058), Dst Port: http (80), Seq: 17756, Ack: 19840, Len: 898  
Hypertext Transfer Protocol  
eXtensible Markup Language

0000 08 01 75 00 00 13 21 57 e8 f9 00 0c f1 0c 30 90 ..u...!W .....0.  
0010 00 11 09 9b 6a 58 80 83 aa aa 03 00 00 00 08 00 .....jX.....  
0020 45 00 03 aa 02 e0 40 00 80 06 f6 fa 0a 3e 20 fe E....@.....>..  
0030 cf 2e 03 09 04 22 00 50 70 f8 2f 4b 4c 8f 8b 78 .....P b./KL...x

File: "/root/public/ipw-May-13-2006-3.dump" 1973 KB 00:11:30 P: 17983 D: 99 M: 0

# WEP Kırma Araçları..

- \*\*\*

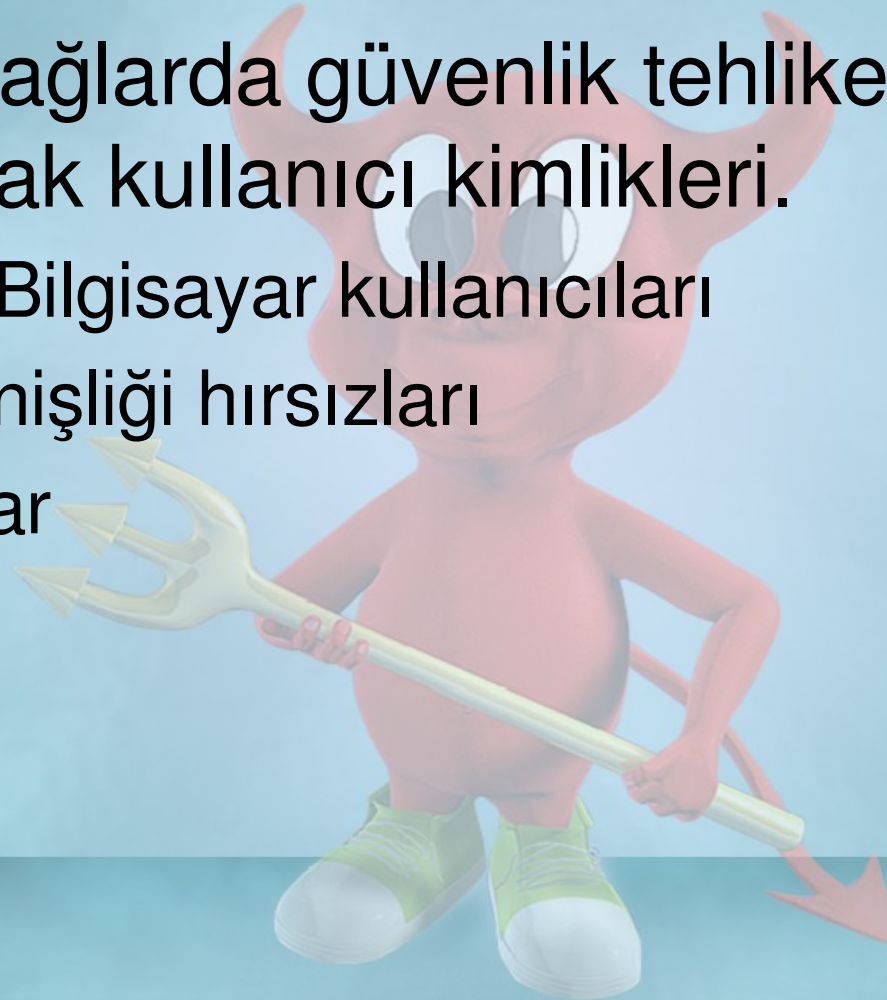


# Nasıl Korunacağız ?

- Kimlerden Korunmalı?
- Ev Kullanıcıları
- İşyerleri
- Halka açık kablosuz ağlar, ya da komşunuzun kablosuz ağı 😊

# Kimlerden Korunmalı?

- Wireless ağlarda güvenlik tehlikesi oluşturacak kullanıcı kimlikleri.
  - Merakli Bilgisayar kullanıcıları
  - Bandgenişliği hırsızları
  - Hackerlar





# Ev Kullanıcıları...

- AP'nin varsayılan SSID'ni değiştirin
- SSID yayınlama iptal edilmeli
- WEP/WPA kullanımı
- MAC tabanlı erişim kontrolü..
- Ağ izleme yazılımı ile kontrol

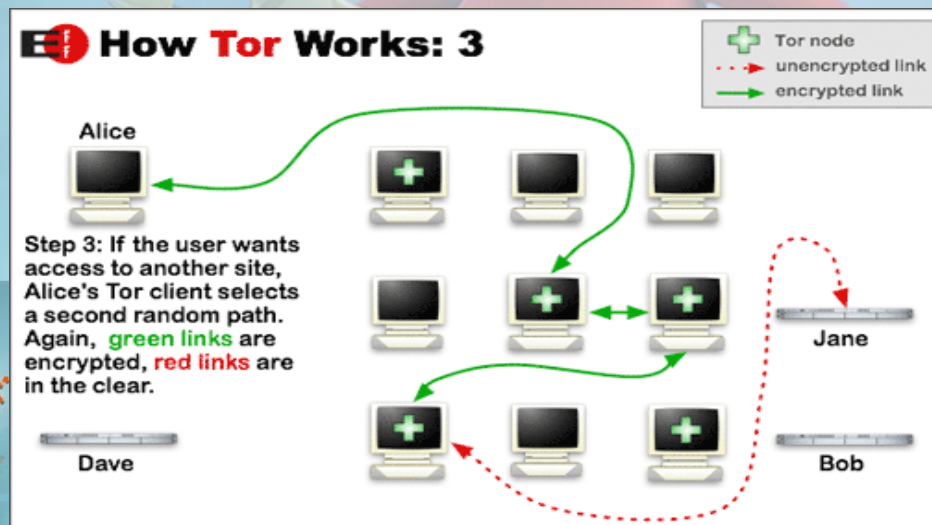
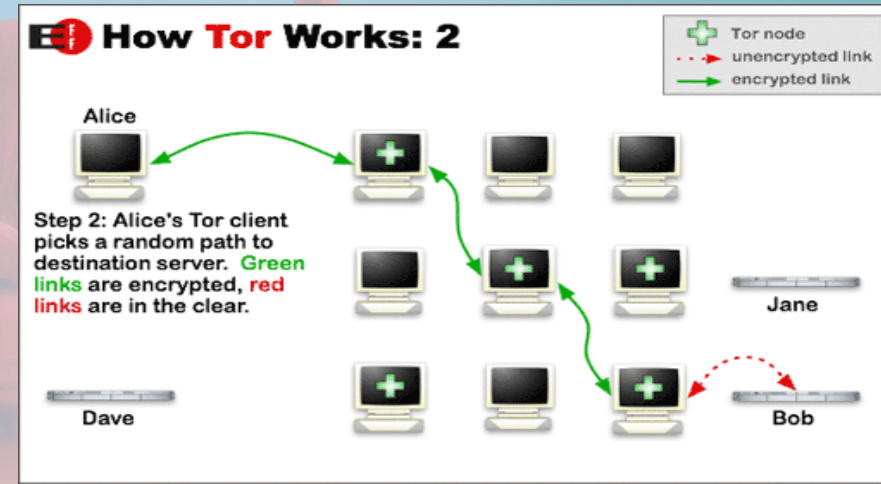
# Şirket Ağları..

- MAC tabanlı erişim kontrolü
  - MAC adres değişimlerinden haberdar olma
- Kullanıcı onaylama / EAP
  - LDAP, Radius vs
- Wireless IDS ile trafik gözleme
- WPA ve güçlü anahtar kullanımı

# Halka açık Kablosuz Ağlar..

- Bilinçli kullanılmazsa yüksek risk içeriyor.
- Ortamdaki kötü niyetli biri tüm trafiği dinleyebilir, değiştirebilir..
- Güvenli kullanım için,
  - TOR Kullanın
  - VPN kullanın

# TOR ile Güvenli Sörf!





# Sonuç..

- Kablosuz ağlarda güvenlik çeşitli protokoller sayesinde giderilsede bu ağları yöneten sistem yöneticileri eğitilmedikçe güvenlik riski her zaman var olacaktır!
- Açık Akademi Güvenlik Kitapları
  - TCP/IP Ağ Güvenliği
  - Ağ Güvenliği İpuçları

# TEŞEKKÜRLER

Bu sunumun en güncel halini  
[www.enderunix.org/slides](http://www.enderunix.org/slides) adresinde  
bulabilirsiniz.

**HUZEYFE ÖNAL**  
[www.enderunix.org/huzeyfe](http://www.enderunix.org/huzeyfe)