

****The best way to stop a criminal is to think the way a criminal thinks****

Güvenlik Testlerinde Açık Kodlu Araçların Kullanımı

Huzeyfe ÖNAL

<http://www.lifeoverip.net>

huzeyfe@lifeoverip.net

Sunum Planı

- Neden güvenlik testleri?
- Açık kod güvenlik test standartları
- Zayıflık Tarama ve Değerlendirme Araçları
- Router/Firewall/IDS/IPS Test araçları
- Yerel Ağlarda güvenlik analizi
- Kablosuz Ağ Güvenliği Testleri

Güvenlik Testlerinde Amaç

- Korumakla sorumlu olduğumuz sistemler
 - 1000 UNIX server? 100 Linux? 1 Windows? Kredi Kartları?
- Korunma için önlemlerim yeterli mi?
 - Firewall, ips, SSL vs
 - Kullanıcı bilinc seviyesi
- Başka bir gözle bakmak
- %99 güvelik = %100 tehlike olabilir

Tanımlar

- Penetrasyon Testleri
 - Black-box
 - White-box
 - Gray-box
- Vulnerability Assessment
- Audit
- False Positive/Negative
- PCI, S-O-X vs

Test Standartları...

- The Open Source Security Testing Methodology Manual (OSSTMM)
- National Institute of Standards and Technology Penetration testing in Special -Publication 800-42
- Information Systems Security Assessment Framework (ISSAF)
- Open Web Application Security Project (OWASP) Framework
-



OWASP TESTING
GUIDE
2007 v2



ISECOM

OSSTMM 2.2.

Open-Source Security Testing Methodology Manual

Created by Pete Herzog

Test Aşamaları..

- Planlama ve Hazırlık
- Değerlendirme(aksiyon süreci)
- Raporlama & Artıkları kaldırma

Planlama Safhası

- Teste dahil edilecek uygulamalar ve ip aralıklarının belirlenmesi
- Test esnasında olusabilecek problemlere karşı ilgili birimlerin yöneticilerinin bilgilendirilmesi
- Sağlam, şartları kesin NDA imzalamak
- Test öncesi gereksinimleri net belirleyen bir RFP hazırlanması
- Test yapan firmanın beceri degerlendirmesi için honeypot sistemler kurulabilir
- Pentest firması seçimi

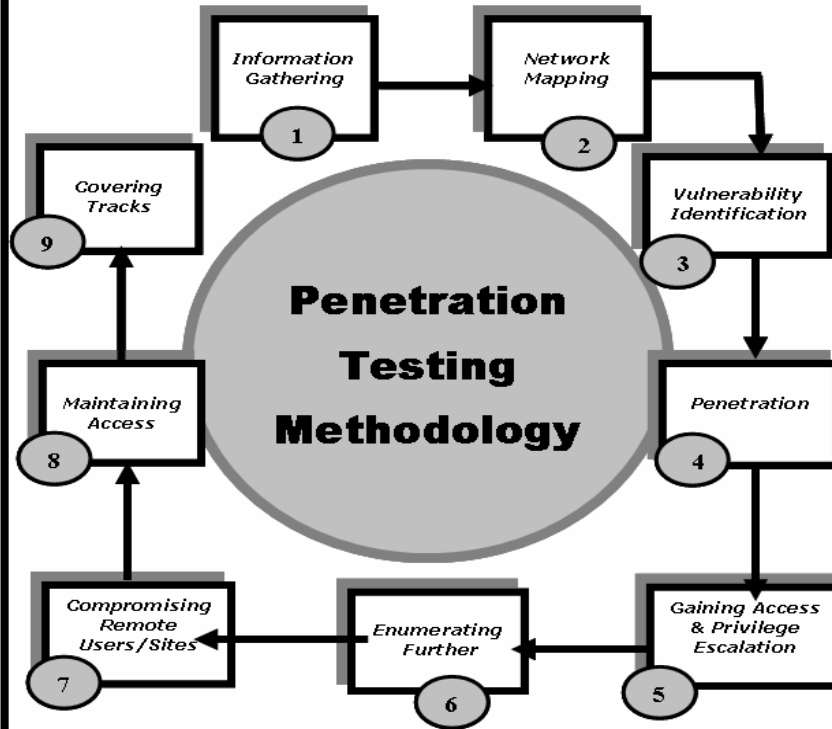
Değerlendirme Sahfası

- Bilgi toplama
- Network haritası çıkarma
- Zayıflık ve açıklıkların belirlenmesi
- Penetrasyon
- Sisteme erişim ve hak yükseltme
- Detaylı araştırma
- Erişilemeyen sistemlere atlama(kopru modu)
- Yapılan erişimleri yönetme
- İzleri temizleme

(1) Planning & Preparation

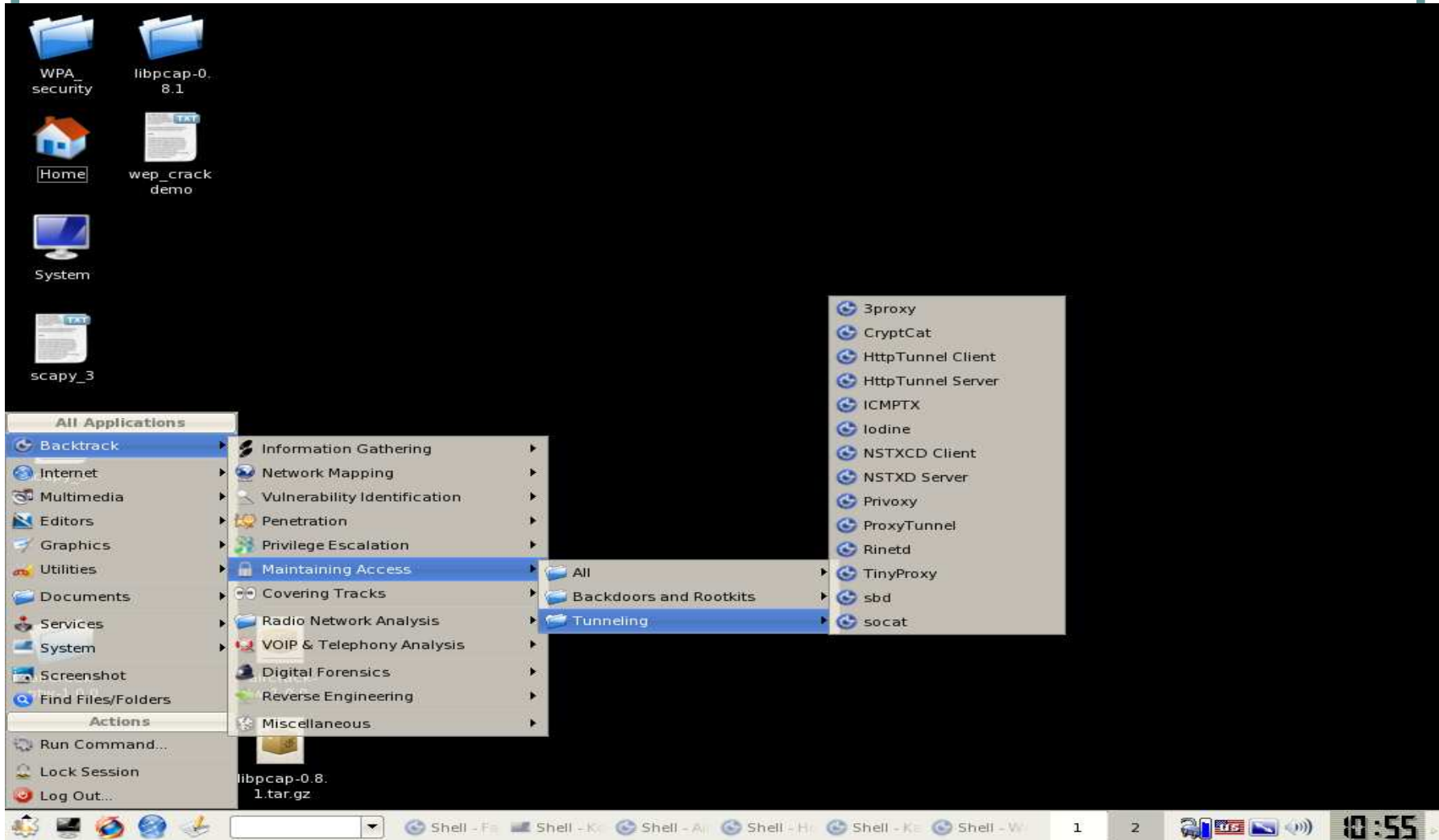
(2)

**A
S
S
E
S
S
M
E
N
T**



(3) Reporting, Clean Up and Destroy Artifacts

Açık kod Test Araçları



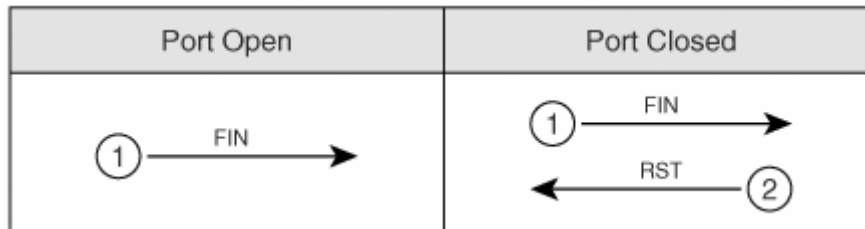
Keşif Süreci

● Pasif Keşif

- E-posta listeleri, ilan siteleri, netcraft , arama motorları

● Aktif Keşif

- Samspace, dig/nslookup, whois, nmap, mail başlıkları



Ağ Haritası Çıkarma

- Aktif IP adreslerinin belirlenmesi
- İşletim sistemleri belirlenme süreci
- Çalışan servislerin bulunması
 - Servis sürüm numaraları
 - Nmap -sV , amap
- Nmap, Xprobe2, tcptraceroute

Zayıflık Tarama :Nessus

- '98 yılında Renaud Deraison tarafından GPL olarak başlatıldı
- İstemci sunucu mimarisine göre çalışır
- Uzak ve yerel sistem güvenliği kontrolü
- KB(Knowledge Base) Destegi
- Web, GUI , konsol ile kolay yönetim
- Güncel zayıflık veritabanı(günlük)
- Bulunan açıklar için detaylı bilgi ve referans
- 15000~ açıklık tanıma imzası
- NASL ile zayıflık tanımlama özelliği

Exploit Geliştirme Altyapısı

The screenshot displays a Metasploit Framework Web Console interface in Mozilla Firefox. The browser address bar shows `http://127.0.0.1:55555/`. The main content area is titled "Microsoft RPC DCOM Interface Overflow" and shows the "CURRENT CONFIGURATION - CHANGE" section. The configuration includes:

- Exploit: `windows/dcerpc/ms03_026_dcom`
- Payload: `windows/adduser/reverse_http`
- Target: `Windows NT SP3-6a/2000/XP/2003 Universal`

Below the configuration is the "OPTIONS" section with the following fields:

OPTION	Required	Value
RHOST	Required	192.168.0.3
RPORT	Required	135
EXITFUNC	Required	

The interface also shows a "Done" button and a "Tor Disabled" status indicator. In the background, a terminal window displays network traffic logs for the same IP address and port.

İçeriden Gelen Saldırıları

- Yerel Ağ bileşenlerinin zayıflıklarından yararlanır. (Switch, Hub, Router)
 - IP spoofing, Mac Spoofing, DNS spoofing
 - Ağa izinsiz giren(Wire/less) saldırgan..
 - Şifresiz İletişimleri izleme, müdahale
- Potansiyel suçlu kitleleri!
 - Patronuna kızan çalışan!
 - Meraklı, bilgili bilgisayar kullanıcıları
- Korunma Yöntemleri..
 - Mac security, VLAN Yapısı, Şifreli iletişim

LAN Saldırı Araçları..

- Trafik Dinleme Araçları: Wireshark, snort, tcpdump
- Şifreli, şifresiz oturumlara müdahale
 - Ettercap

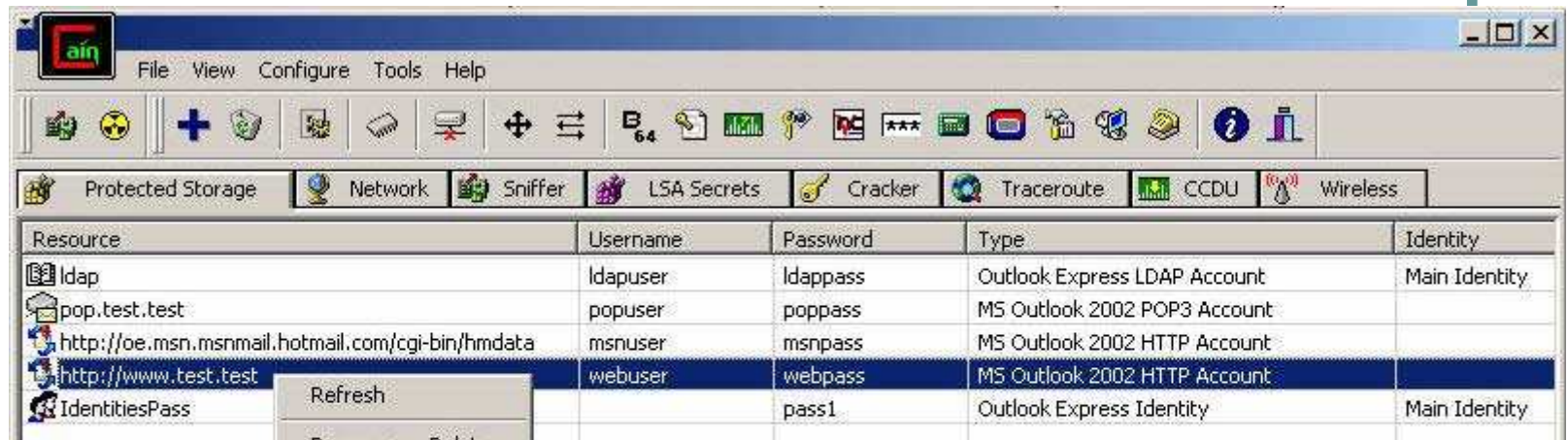
```
ettercap 0.6.7
Filter: OFF
doppleganger - illithid (ARP Based) - ettercap
Active Dissector: ON

20 hosts in this LAN (192.168.0.246 : 255.255.255.0)
1) 192.168.0.32:1050 <--> 212.168.15.125:80      UDP      http
2) 192.168.0.31:1049 <--> 192.168.0.200:1900  UDP
3) 192.168.0.32:1057 <--> 212.168.15.195:80   silent   http
4) 192.168.0.61:1130 <--> 210.255.65.2:80     silent   http
5) 192.168.0.22:1032 <--> 192.168.0.200:1900  UDP
6) 192.168.0.54:2590 <--> 212.5.174.159:53   UDP      domain
7) 192.168.0.54:2590 <--> 212.45.15.10:53    UDP      domain
8) 192.168.0.54:2591 <--> 212.45.15.10:53    UDP      domain
9) 192.168.0.54:2591 <--> 212.5.174.159:53   UDP      domain

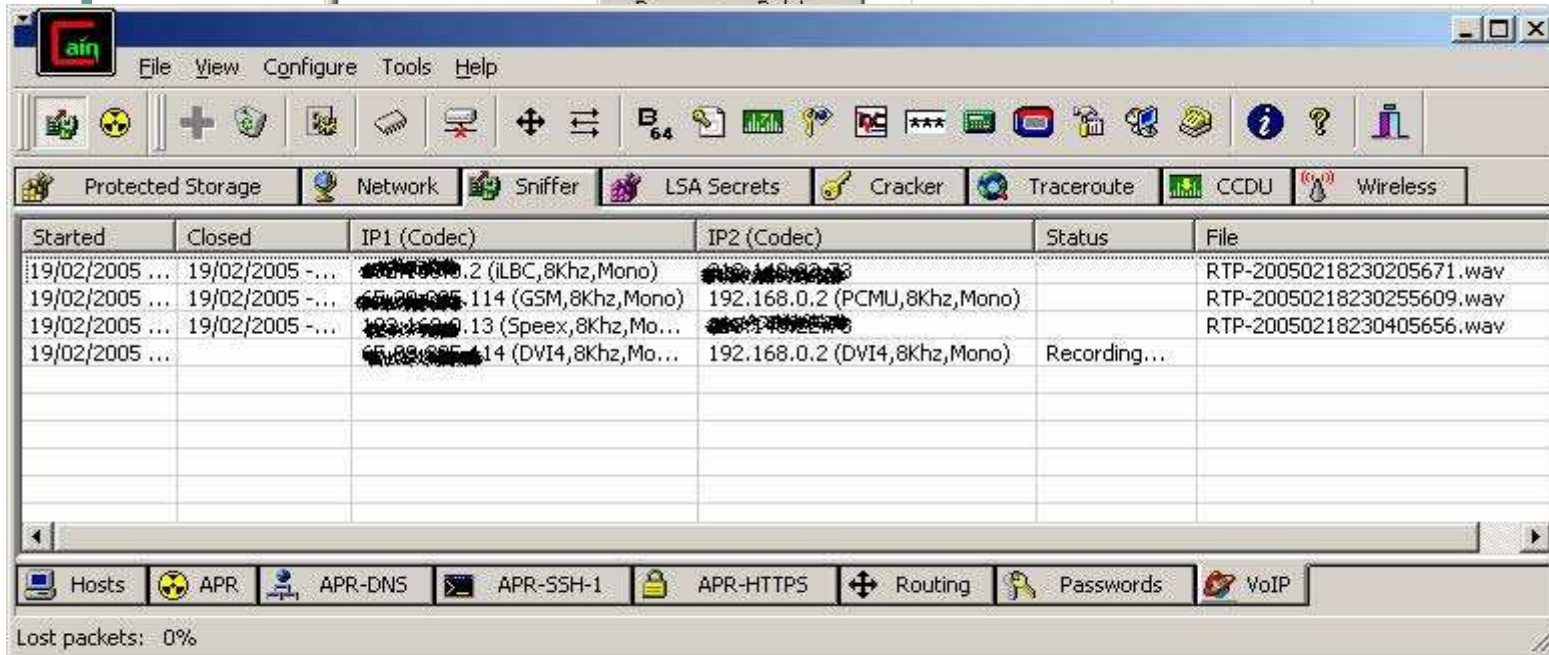
Your IP: 192.168.0.246 MAC: 00:00:21:12:84:1F Iface: dev1 Link: HUB
```

- İsviçre Çakısı: Cain & Abel

Cain & Abel



Resource	Username	Password	Type	Identity
ldap	ldapuser	ldappass	Outlook Express LDAP Account	Main Identity
pop.test.test	popuser	poppass	MS Outlook 2002 POP3 Account	
http://oe.msn.msnmail.hotmail.com/cgi-bin/hmdata	msnuser	msnpass	MS Outlook 2002 HTTP Account	
http://www.test.test	webuser	webpass	MS Outlook 2002 HTTP Account	
IdentitiesPass		pass1	Outlook Express Identity	Main Identity



Started	Closed	IP1 (Codec)	IP2 (Codec)	Status	File
19/02/2005 ...	19/02/2005 - ...	192.168.0.2 (iLBC,8Khz,Mono)	192.168.0.2 (PCMU,8Khz,Mono)		RTP-20050218230205671.wav
19/02/2005 ...	19/02/2005 - ...	192.168.0.114 (GSM,8Khz,Mono)	192.168.0.2 (PCMU,8Khz,Mono)		RTP-20050218230255609.wav
19/02/2005 ...	19/02/2005 - ...	192.168.0.13 (Speex,8Khz,Mo...)	192.168.0.2 (PCMU,8Khz,Mono)		RTP-20050218230405656.wav
19/02/2005 ...		192.168.0.14 (DVI4,8Khz,Mo...)	192.168.0.2 (DVI4,8Khz,Mono)	Recording...	

Hosts APR APR-DNS APR-SSH-1 APR-HTTPS Routing Passwords VoIP

Lost packets: 0%

HTTPS Trafigi Degistirme

The screenshot shows the MSN Hotmail sign-in page in a Mozilla Firefox browser window. The browser's address bar displays the URL: <http://login.live.com/login.srf?id=2&svc=mail&cbid=24325&msppjph=1&tw=0&fs=1&fsa=1&fsat=1296000&lang=EN&lc=1033>. The page features the MSN logo and the text "Hotmail". A navigation bar includes links for "Home", "My MSN", "Shopping", "Money", and "People & Chat", along with a search box. A prominent message reads: "What's new For Free Hotmail? MSN Hotmail Inbox Storage is now 250 MB and there is an increased attachment size of 10 MB!". Below this, a section titled "New to MSN Hotmail? A smarter way to email – FREE!" lists several benefits: enhanced security, easy connection, and personalization. A "Sign Up" button is provided. The main sign-in area, titled "Sign In to Hotmail", contains fields for "E-mail address" (filled with "rastgele@hotmail.com") and "Password" (filled with "*****"). A "Sign In" button is located below these fields. To the right of the sign-in form, there are radio button options: "Save my e-mail address and password" (selected), "Save my e-mail address", and "Always ask for my e-mail address and password". A link for "Sign in using enhanced security" is also present. At the bottom of the sign-in area, there is a "Windows Live ID" section with links for "Account Services", "Privacy Statement", and "Terms of Use". The footer of the page includes copyright information: "©2006 Microsoft Corporation" and "MSN Privacy & Legal", along with an "About" link. The browser's status bar at the bottom left shows "Tamam".

HTTPS Trafigi Degistirme

The image shows a web browser window displaying the Hotmail login page. The browser's address bar shows the URL: `http://login.live.com/login.srf?id=2&svc=mail&cbid=24325&msppjph=1&tw=0&fs=1&fsa=1&fsat=1296000&_lang=EN&lc=1033`. The page content includes a search bar, the Hotmail logo, and a sign-in form with fields for "E-mail address" (containing "rastgele@hotmail.com") and "Password" (containing "*****"). There are also radio buttons for saving login information and a "Sign In" button.

Overlaid on the bottom of the browser window is the Paros Proxy tool window, titled "Paros - Untitled Session". The "Request" tab is active, showing the intercepted HTTP request details:

```
POST https://login.live.com/ppsecure/post.srf?id=2&svc=mail&cbid=24325&msppjph=1&tw=0&fs=1&fsa=1&fsat=1296000&_lang=EN&lc=1033&bk=1147582792 HTTP/1.1
Host: login.live.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; tr; rv:1.8.0.3) Gecko/20060426 Firefox/1.5.0.3
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: tr-TR,tr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Charset: ISO-8859-9,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

Parameter Name	Value
PPSX	Pa
PwdPad	IfYouAreReadingThisYouHaveTooM
login	rastgele@hotmail.com
passwd	bugun_pazar
LoginOptions	2
PPFT	Blr3IdQcJswovObWUAdpyM5*f0xK0IecIn92KMPi0Bd55Yh3s7b0721q9BdEweQa5EJ...

At the bottom of the Paros window, a list of intercepted requests is visible:

```
1 GET http://hotmail.com/ HTTP/1.1 => HTTP/1.1 302 Redirected [1.622 s]
3 GET http://lc2.bay0.hotmail.passport.com/cgi-bin/login HTTP/1.1 => HTTP/1.1 302 Redirected [0.711 s]
6 GET http://www.hotmail.com/ HTTP/1.1 => HTTP/1.1 302 Found [0.391 s]
8 GET http://login.live.com/login.srf?id=2&svc=mail&cbid=24325&msppjph=1&tw=0&fs=1&fsa=1&fsat=1296000&_lang=EN HTTP/1.1 => HTTP/1.1 302 Found [0.631 s]
```

Firefox/Internet Explorer?


Sunucu Sertifika Son Tarihi

"Paros" , iletişim esnasında bilgileri şifreleme için bir güvenlik sertifikası kullanan bir bölgedir, fakat sizin sertifikanız 08.11.2002 11:50 tarihinde günü geçmiş.

Bilgisayar saatinizin (şu anda 14 Mayıs 2006 Pazar 08:09:58) doğruluğunu kontrol edin.

Buna rağmen devam edelim mi ?

Ağ sayfası bilinmeyen bir yetkili tarafından onaylanmıştır

 Paros güvenli site olarak kabul edilemiyor.

Olası hata sebepleri:

- Tarayıcınız sertifika hazırlayıcısının hazırladığı sayfa sertifikasını tanımıyor.
- Sayfa sertifikalarının ayarları yanlış veya sertifikanın zamanın geçmiş olabilir.
- Özel bilgilerinize ulaşabilecek ve kendini Paros gibi gösteren bir siteye bağlandınız.

Lütfen sayfa yöneticisine bu sorun hakkında bilgi verin.


Bu sertifikayı kabul etmeden önce sayfanın sertifikacısını araştırıp kontrol etmelisiniz. Paros kimlikli sertifikayı kabul etmeye hazır mısınız?




Bu sertifikayı kalıcı olarak kabul et

Bu sertifikayı sadece bu oturum için kabul et

Bu sertifikayı kabul etme ve bu ağ sayfasına bağlanma

Security Alert

 Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

-  The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
-  The security certificate has expired or is not yet valid.
-  The name on the security certificate is invalid or does not match the name of the site.

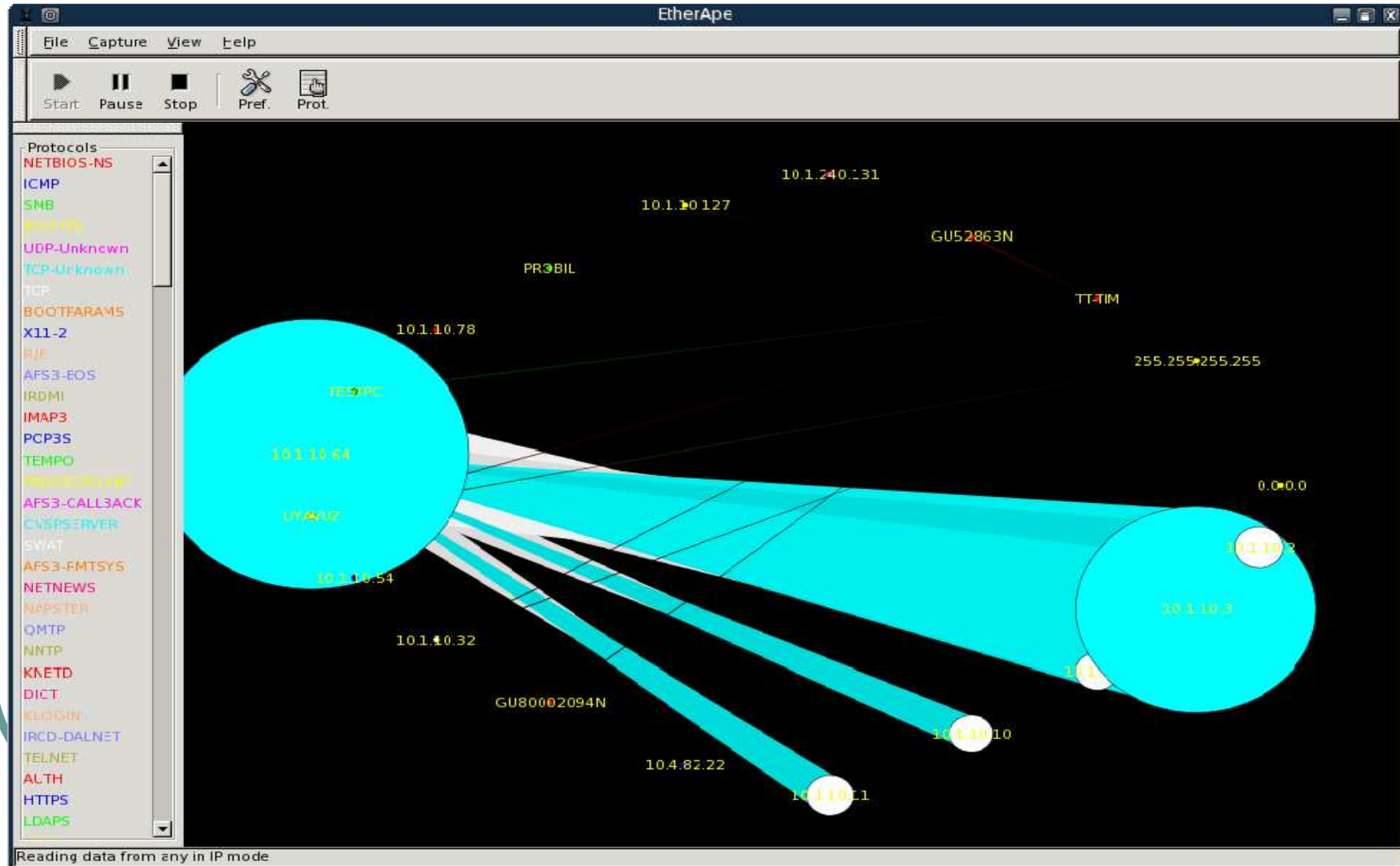
Do you want to proceed?

Güvenlik Hatası: Alan ismi birbirini tutmuyor

"login.live.com" ile bağlantı kurmayı denediniz. Bu sayfayla kurduğunuz iletişimi gizlice izlemeye çalışan sertifika, "Paros" sunucusuna ait değil.

Gösterilen Sertifikanın login.live.com sunucusuna ait olmadığını düşünüyorsanız, bu sayfayla olan bağlantınızı kesin ve ağ yöneticisi ile iletişim kurun.

LAN Trafik Analizi



L2 güvenlik testleri-yersinia

- Bileşenleri: Libnet, libpcap ve ncurses
- Linux, Solaris, *BSD sistemlere asina
- STP, CDP, DTP, DHCP, HSRP, VTP protokollerini destekler
- Cisco benzeri CLI, Ncurses arabirimi
 - Yersinia -D 12000/tcp portunu dinler
 - Yersinia -I Ncurses arabirimi

Yersinia...

```
Shell - Konsole
----- yersinia 0.7 by Slay & tomac - STP mode ----- [09:16:19]
RootId      BridgeId    Port      Iface Last seen
2000.0012446B700A 2000.0012446B700A 8081      eth0 04 May 09:16:16
2000.0012446A700A 2000.0012446A700A 8081      eth0 04 May 09:16:19

----- Attack Panel -----
No  DoS  Description
0   sending conf BPDU
1   sending tcn BPDU
2   X   sending conf BPDUs
3   X   sending tcn BPDUs
4   Claiming Root Role
5   Claiming Other Role
6   X   Claiming Root Role with MiTM

----- Select attack to launch ('q' to quit) -----

----- Total Packets: 37 ----- STP Packets: 20 ----- MAC Spoofing [X] -----
Those strange attacks...
----- STP Fields -----
Source MAC 00:12:DA:89:9C:D0 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 2000.0012446B700A Pathcost 00000000
BridgeId 2000.0012446B700A Port 8081 Age 0000 Max 0014 Hello 0002 Fwd 000F
```

DNS Protokolü Güvenliđi

- Zone transferi

- *\$ dig @<dns_sunucu_adresi> -t AXFR huzeyfe.net*

- Ip -> isim çözümlleme

- Passive DNS replication, PTR

- **# dig @ns1.tekrom.com version.bind chaos txt**

;; ANSWER SECTION:

version.bind. 0 CH TXT "9.2.4"

DNS Cache Snooping

- Gerçek kayıtların arasına sahte dns kayıtları eklemek
- Bu sunucuya sorgu yapan tüm istemci ve cache dns sunucular zehirlenir...
- Dig +trace www.lifeoverip.net
- Dnsa ile gerçekleştirilebilir

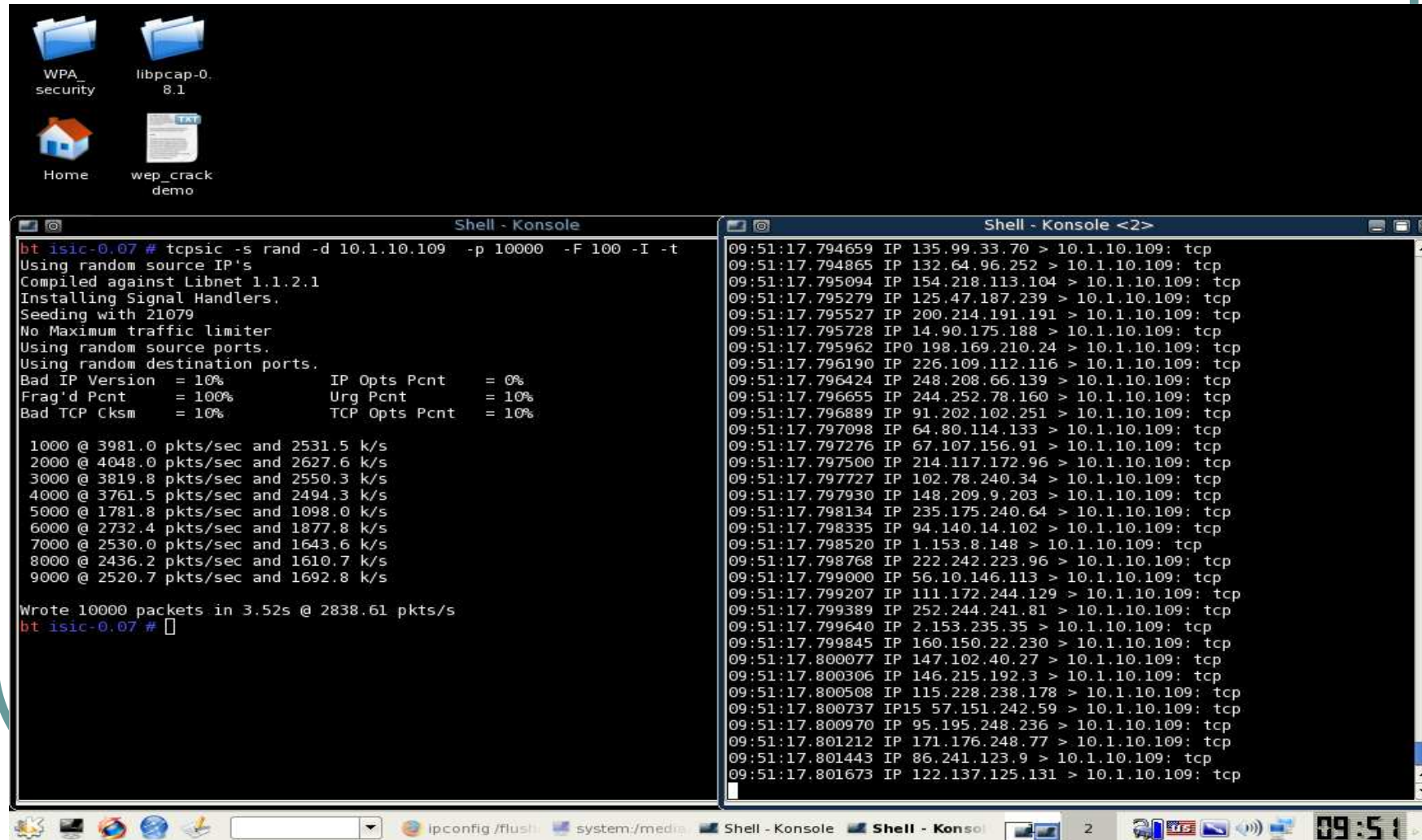
```
huzeyfe.net. 14400 IN NS ns1.tekrom.com.
huzeyfe.net. 14400 IN NS ns2.tekrom.com.

huzeyfe.net. 14400 IN A 67.15.80.71

localhost.huzeyfe.net. 14400 IN A 127.0.0.1

huzeyfe.net. 14400 IN MX 0 mail.lifeoverip.net.
openbsd.huzeyfe.net. 14400 IN A 104.27.72.38
openids.huzeyfe.net. 14400 IN A 104.27.72.38
www 14400 IN A 67.15.122.30
ipsor 14400 IN A 67.15.122.30
plog 14400 IN A 67.15.122.30
blog 14400 IN CNAME plog
#blog 14400 IN A 194.27.72.88
security 14400 IN A 194.27.72.88
netsec 14400 IN A 194.27.72.88
test 14400 IN A 80.93.212.86
tunnel 14400 IN NS test
abc.huzeyfe.net. IN MX 0 test.huzeyfe.net.
com. 300 IN NS mail.lifeoverip.net.
```

Firewall/IDS Performans Testleri



```
bt isic-0.07 # tcpsic -s rand -d 10.1.10.109 -p 10000 -F 100 -I -t
Using random source IP's
Compiled against Libnet 1.1.2.1
Installing Signal Handlers.
Seeding with 21079
No Maximum traffic limiter
Using random source ports.
Using random destination ports.
Bad IP Version = 10%      IP Opts Pcmt = 0%
Frag'd Pcmt = 100%      Urg Pcmt = 10%
Bad TCP Cksm = 10%      TCP Opts Pcmt = 10%

1000 @ 3981.0 pkts/sec and 2531.5 k/s
2000 @ 4048.0 pkts/sec and 2627.6 k/s
3000 @ 3819.8 pkts/sec and 2550.3 k/s
4000 @ 3761.5 pkts/sec and 2494.3 k/s
5000 @ 1781.8 pkts/sec and 1098.0 k/s
6000 @ 2732.4 pkts/sec and 1877.8 k/s
7000 @ 2530.0 pkts/sec and 1643.6 k/s
8000 @ 2436.2 pkts/sec and 1610.7 k/s
9000 @ 2520.7 pkts/sec and 1692.8 k/s

Wrote 10000 packets in 3.52s @ 2838.61 pkts/s
bt isic-0.07 #
```

```
09:51:17.794659 IP 135.99.33.70 > 10.1.10.109: tcp
09:51:17.794865 IP 132.64.96.252 > 10.1.10.109: tcp
09:51:17.795094 IP 154.218.113.104 > 10.1.10.109: tcp
09:51:17.795279 IP 125.47.187.239 > 10.1.10.109: tcp
09:51:17.795527 IP 200.214.191.191 > 10.1.10.109: tcp
09:51:17.795728 IP 14.90.175.188 > 10.1.10.109: tcp
09:51:17.795962 IP 198.169.210.24 > 10.1.10.109: tcp
09:51:17.796190 IP 226.109.112.116 > 10.1.10.109: tcp
09:51:17.796424 IP 248.208.66.139 > 10.1.10.109: tcp
09:51:17.796655 IP 244.252.78.160 > 10.1.10.109: tcp
09:51:17.796889 IP 91.202.102.251 > 10.1.10.109: tcp
09:51:17.797098 IP 64.80.114.133 > 10.1.10.109: tcp
09:51:17.797276 IP 67.107.156.91 > 10.1.10.109: tcp
09:51:17.797500 IP 214.117.172.96 > 10.1.10.109: tcp
09:51:17.797727 IP 102.78.240.34 > 10.1.10.109: tcp
09:51:17.797930 IP 148.209.9.203 > 10.1.10.109: tcp
09:51:17.798134 IP 235.175.240.64 > 10.1.10.109: tcp
09:51:17.798335 IP 94.140.14.102 > 10.1.10.109: tcp
09:51:17.798520 IP 1.153.8.148 > 10.1.10.109: tcp
09:51:17.798768 IP 222.242.223.96 > 10.1.10.109: tcp
09:51:17.799000 IP 56.10.146.113 > 10.1.10.109: tcp
09:51:17.799207 IP 111.172.244.129 > 10.1.10.109: tcp
09:51:17.799389 IP 252.244.241.81 > 10.1.10.109: tcp
09:51:17.799640 IP 2.153.235.35 > 10.1.10.109: tcp
09:51:17.799845 IP 160.150.22.230 > 10.1.10.109: tcp
09:51:17.800077 IP 147.102.40.27 > 10.1.10.109: tcp
09:51:17.800306 IP 146.215.192.3 > 10.1.10.109: tcp
09:51:17.800508 IP 115.228.238.178 > 10.1.10.109: tcp
09:51:17.800737 IP 57.151.242.59 > 10.1.10.109: tcp
09:51:17.800970 IP 95.195.248.236 > 10.1.10.109: tcp
09:51:17.801212 IP 171.176.248.77 > 10.1.10.109: tcp
09:51:17.801443 IP 86.241.123.9 > 10.1.10.109: tcp
09:51:17.801673 IP 122.137.125.131 > 10.1.10.109: tcp
```

WLAN Güvenliđi

- Keşif Araçları
- WEP güvenlik testi
- WPA güvenlik testi
- Sahte AP komlandırımı
- WLAN Pentest aracı

Pasif Keşif: Kismet

The screenshot shows a Linux desktop with a dark theme. On the left side, there are several files: 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, and ipw-Apr-30-2006-1.xml. The main window is titled "Kismet eth1" and displays a network list and status information.

Network List (Autofit)

Name	Clnt	T	W	Ch	Rate	SignalGraph	Nse	Pckts	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	D2	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	D4	144.122.5.183	24k	0	0
! misafir	22	A	N	001	36.0		-25	185	D2	144.122.0.0	8k	0	0
! misafir	21	A	N	005	36.0		-25	321	D4	144.122.5.183	8k	0	0
! misafir	1	A	N	005	36.0		0	4	U4	10.62.33.252	108B	0	0
! misafir	0	A	N	001	36.0		0	1	T4	144.122.4.12	0B	0	0
-Go ssid	0	A	N	007	54.0		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

Networks: 11
Packets: 2123
Cryptd: 3
Weak: 0
Noise: 5
Discard: 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 144.122.5.174 for misafir:00:12:F0:31:20:FD via ARP
Found IP 144.122.4.23 for misafir:00:13:DE:27:2A:21 via TCP
Found IP 144.122.5.92 for misafir:00:12:F0:61:91:B9 via UDP

Battery: unavailable

The taskbar at the bottom shows the system tray with icons for network, volume, and power, and the system clock displaying 12:25.

Kismet – AP Kesfi

```
Network List (SSID)
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:BF: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

Hızlı WEP Key bulma:aircrack-ptw

```
root@wirelessdefence:/  
File Edit View Terminal Tabs Help  
[root@wirelessdefence /]# airodump-ng --channel 11 --write Apr 07 ath0
```

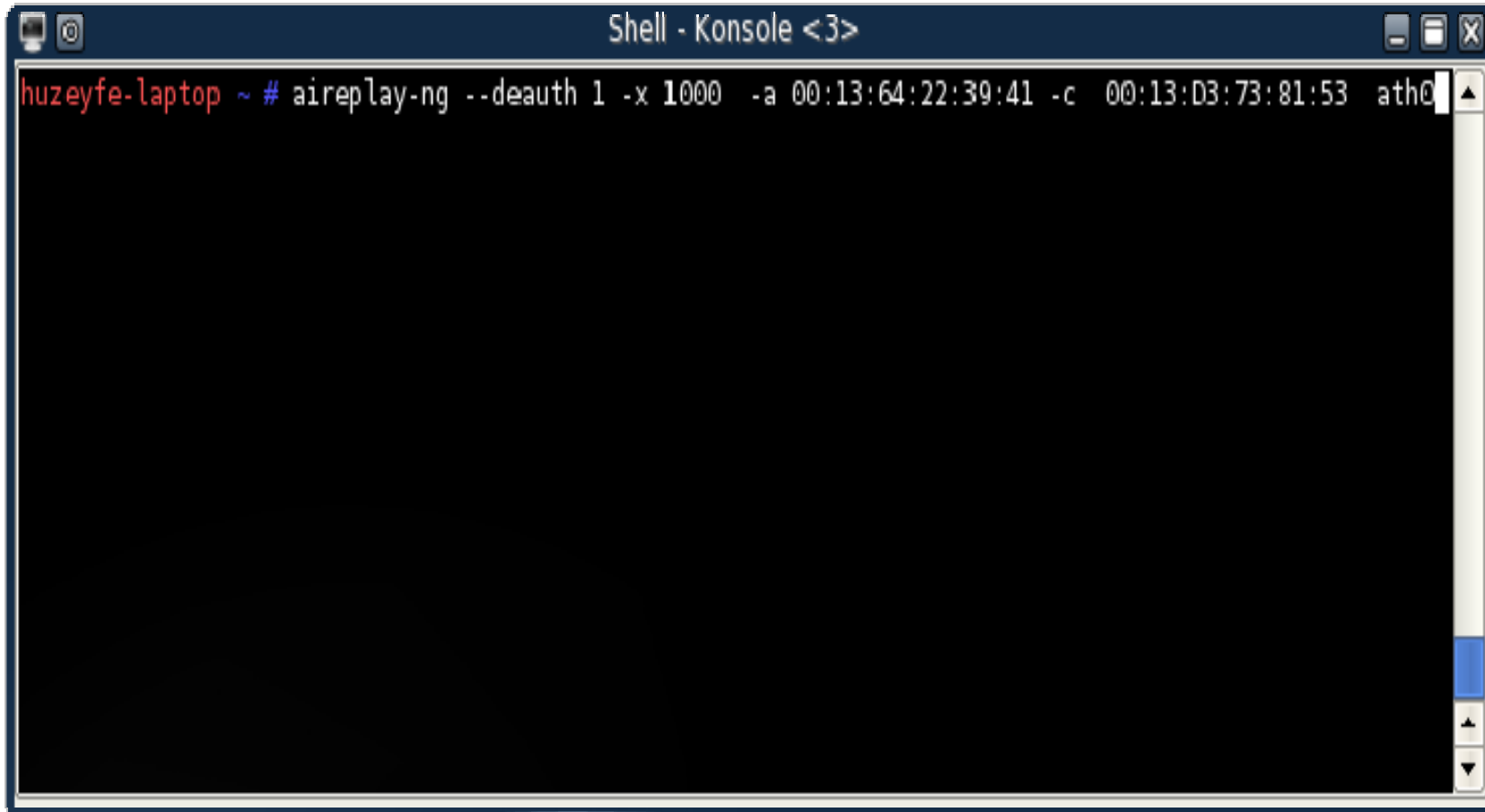
```
root@wirelessdefence:/  
File Edit View Terminal Tabs Help  
CH 11 ][ BAT: 2 hours 52 mins ][ Elapsed: 8 mins ][ 2007-04-05 23:32  
  
BSSID          PWR  Beacons  # Data  CH  MB  ENC  ESSID  
00:12:17:A7:AF:E4  49    5054    41289  11  54. WEP  linksys-g  
  
BSSID          STATION          PWR  Packets  Probes  
00:12:17:A7:AF:E4  00:0F:3D:57:FD:C0  39   44515
```

```
root@wirelessdefence:/tools/wifi/aircrack-ptw-1.0.0  
File Edit View Terminal Tabs Help  
[root@wirelessdefence aircrack-ptw-1.0.0]# ./aircrack-ptw /Apr07-02.cap  
This is aircrack-ptw 1.0.0  
For more informations see http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/  
allocating a new table  
bssid = 00:12:17:A7:AF:E4  keyindex=0  
stats for bssid 00:12:17:A7:AF:E4  keyindex=0 packets=11  
[root@wirelessdefence aircrack-ptw-1.0.0]#
```

WPA Crack – auth. paketi yakalama

```
Shell - Konsole <2>
CH 11 ][ Elapsed: 17 mins ][ 2007-02-24 14:55 ][ 2007-02-24 14:38
BSSID          PWR  Beacons  # Data  CH  MB  ENC  ESSID
00:13:64:22:39:41 135    5122    96789  11  54. WPA  S-Guard
BSSID          STATION      PWR  Packets  Probes
00:13:64:22:39:41 00:13:D3:73:81:53 135    97029
huzeyfe-laptop ~ # airodump-ng --channel 11 --write wpa_crack ath0
```

WPA Crack – Ağdan düşürme



```
Shell - Konsole <3>
huzeyfe-laptop ~ # aireplay-ng --deauth 1 -x 1000 -a 00:13:64:22:39:41 -c 00:13:D3:73:81:53 ath0
```

The image shows a terminal window titled "Shell - Konsole <3>". The prompt is "huzeyfe-laptop ~ #". The command entered is "aireplay-ng --deauth 1 -x 1000 -a 00:13:64:22:39:41 -c 00:13:D3:73:81:53 ath0". The terminal is otherwise empty.

WPA Crack – PSK kırma

```
Shell - Konsole
Aircrack-ng 0.6.2

[00:00:00] 46 keys tested (48.61 k/s)

KEY FOUND! [ test1234 ]

Master Key      : 99 5D 77 7F DE 90 E4 11 B1 8E 94 6D A0 17 DD 3E
                  D0 A7 04 1B 64 A3 60 19 B2 93 8E AA B3 34 30 AE

Transient Key   : 2E 47 26 62 58 79 F2 A5 8F A1 8D 47 4A 26 50 47
                  51 6F 32 8C D0 2E E3 E3 B4 68 90 0B 1C 3A F8 03
                  23 A0 5A B5 CB 56 09 FF 8A F5 1B 90 5F 68 98 76
                  30 FF 49 71 FF CE 6B A5 2F D9 E6 BB FD 2E 29 56

EAPOL HMAC     : CE 6A 13 7A CC 42 2C 38 D1 5C DB 63 60 E1 8D 08

huzeyfe-laptop ~ # aircrack-ng -a 2 -b 00:13:64:22:39:41 -w /tmp/wordlist wpa_crack-01.cap
```

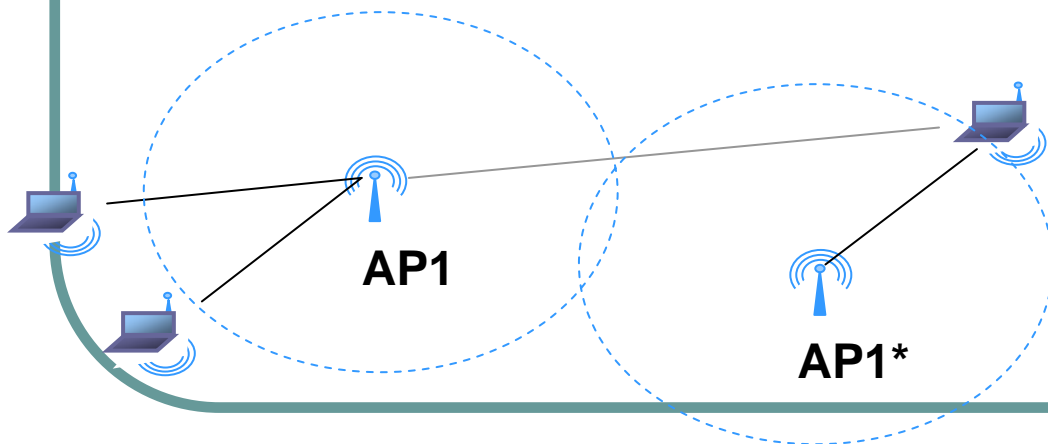
Sahte AP(Erisim Noktalari)

```
root@wirelessdefence:/tools/wifi/fakeap-0.3.2
File Edit View Terminal Tabs Help
[root@wirelessdefence fakeap-0.3.2]# perl fakeap.pl --interface wlan0 --words lists/stefan-wordlist.txt --vendors lists/stefan-maclist.txt

fakeap 0.3.1 - Wardriving countermeasures
Copyright (c) 2002 Black Alchemy Enterprises. All rights reserved

Using interface wlan0:
Generating ESSIDs from lists/stefan-wordlist.txt
Using 53068 words for ESSID generation
Using 20 vendors for MAC generation

-----
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig55: ESSID=grate          chan=10 Pwr=Def WEP=N MAC=00:07:20:c2:30:85
```



MAC	SSID	Chan	Speed	Type	Enc...
0000CEB8D54F	BANANA	11	11 Mbps	AP	WEP
0000C0B9F8B	BANANA	11	11 Mbps	AP	WEP
0000C72FFC8	BANANA	11	11 Mbps	AP	WEP
0000C8AE489	BANANA	11	11 Mbps	AP	WEP
0000C361C75	BANANA	11	11 Mbps	AP	WEP
0000C1FA804	BANANA	11	11 Mbps	AP	WEP
0000CE022FC4	BANANA	11	11 Mbps	AP	WEP
0000CCB8DD6	BANANA	11	11 Mbps	AP	WEP
0000CE579BE7	BANANA	11	11 Mbps	AP	WEP
0000C5BC03C	BANANA	11	11 Mbps	AP	WEP
0000C76DE04	BANANA	11	11 Mbps	AP	WEP
0000CB07399	BANANA	11	11 Mbps	AP	WEP
0000CE6128F6	BANANA	11	11 Mbps	AP	WEP
0000C37AD95	BANANA	11	11 Mbps	AP	WEP
0000CE11EF14	BANANA	11	11 Mbps	AP	WEP
0000CE9A74CB	BANANA	11	11 Mbps	AP	WEP

Wi-fi Pentest - Wicrawl

The screenshot displays the Wicrawl application window. The interface includes a menu bar (File, Edit, View, Wicrawl, Tabs), a toolbar with icons for Start, Plugins, Interfaces, Profiles, and Minimize, and an SSID Filter input field. Two tabs are visible: 'AP Information' and 'Plugin Information'. The 'AP Information' tab contains a table with the following data:

SSID	BSSID	Time	Packets	Plugin	Event	Timestamp	Encryption	Power	Channel
linksys	00:06:25:54:a6:c1	0	0	DHCP	associated	3-7-2006 13:17:8	None	0	00
Frog	00:0f:66:95:a0:bd	0	0	iwconfig association	new-ap	3-7-2006 13:18:25	None	0	00
wi-foo	00:12:17:28:15:5b	0	0	Internet Speed Check	have-internet	3-7-2006 13:18:8	WEP	0	11
kenswireless	00:13:10:d2:d0:ec	0	0	iwconfig association	new-ap	3-7-2006 13:18:25	None	0	11

Below the table is an 'Output' section with a scrollable log area containing the following text:

```
[ - ] Found no new APs in discovery, I'll wait a bit more...  
(last count [4] new count [4])  
[ - ] Found no new APs in discovery, I'll wait a bit more...  
(last count [4] new count [4])  
[ - ] Found no new APs in discovery, I'll wait a bit more...  
(last count [4] new count [4])  
Stop was pressed  
Killing child [25481]  
Child [25481] dead  
Discovery and plugin-engine finished
```

Wicrawl Eklentileri

wicrawl plugins

Please feel free to add a new row with the status set to "Requested" if you have a good idea or a request for a plugin.

plugin name	description	status
aircrack-wep-cracking	Crack WEP encryption with the use of aircrack-ng	Done
check_internet	Checks internet connectivity (by way of icmp)	Done
check_speed	Checks latency of your connection	Done
cowpatty-wpa-psk-bruteforce	Uses coWPAtty to try to brute force the pre-shared-key for WPA	Done
dhcp	Uses DHCP to get an address on the local network	Done
example-bash	Example (template) plugin written in bash	Done
example-perl	Example (template) plugin written in perl	Done
example-fortran	Example (template) plugin written in fortran ;)	Done
ext_ip	Checks to see what your external IP is	Done
gpsd	Gets your GPS coordinates through GPSd	Done
hold_internet	Tries to hold your internet connection.	Done
isassociated	Checks to see whether you're associated or not	Done
iwconfig_associate	uses iwconfig to see whether you're associated to an AP or not	Done
nessus	Runs nessus against the AP (or default gw) (requires configuration)	Done
nmap_plugin	Runs nmap against the network to see what hosts are up	Done
pickupline	Attempts to bypass captive portals by assuming the identity of a local network user	Done
random_mac	randomizes your mac address before you connect	Done
rogue_ap_check	Checks to see if this AP is connected to your network by connecting to a known server	Done
text_to_speech	Announces new access points or internet connectivity	Done
wep-lab-bruteforce	Tries to bruteforce the WEP password	Done
MAC Manuf Detect	Gives the manufacturer of the Access Point	In CVS
Amaaa fui Plugin for LINUX	Text UI	Incomplete
aircrack-ptw	Crack WEP encryption with the use of the new ptw attack	Requested

TEŐEKKÜRLER

Bu sunumun en güncel halini
www.lifeoverip.net/slides adresinde
bulabilirsiniz.

HUZEYFE ÖNAL
huzeyfe@lifeoverip.net
www.lifeoverip.net