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?
- Açıkkod 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..

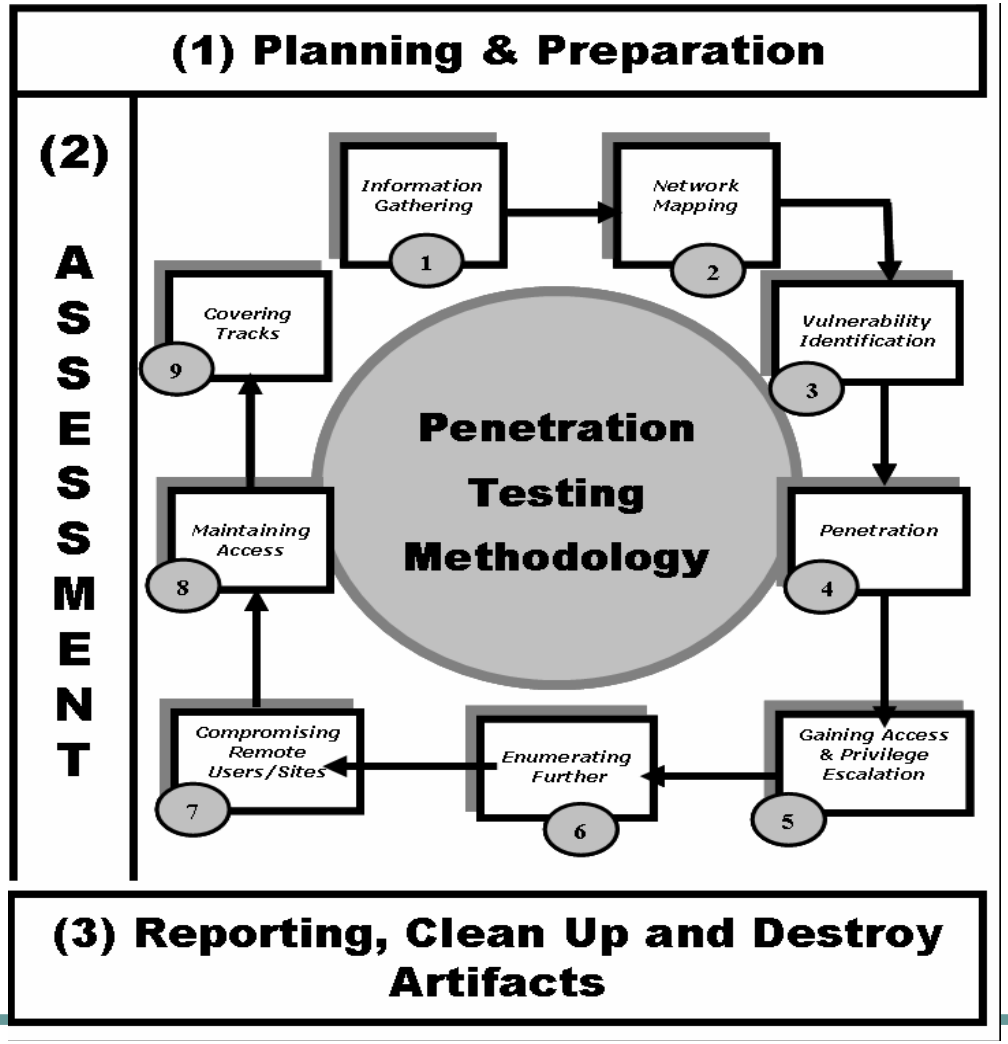
- Planlama ve Hazırlık
- Değerlendirme(aksiyon süreci)
- Raporlama & Artıkları kaldırma

Planlama Safhası

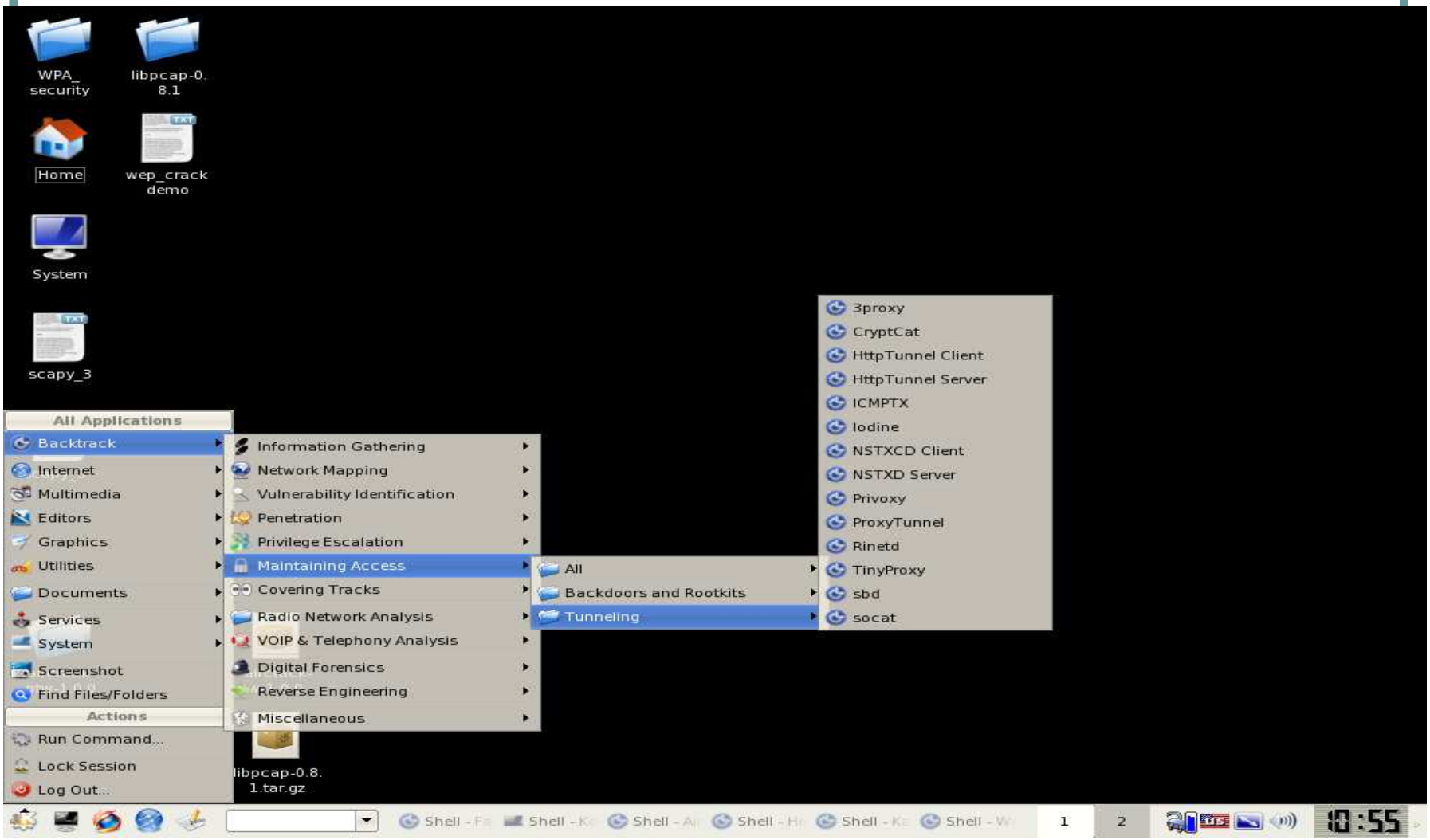
- Teste dahil edilecek uygulamalar ve ip aralıklarınınbelirlenmesi
- Test esnasında olusabilecek problemlere karşı ilgli birimlerin yöneticilerinin bilgilendirilmesi
- Sağlam, şartları kesin NDA imzalamak
- Test öncesi gereksinimleri net belirleyen bir RFP hazırlanması
- Test yapan firmanın beceri degerlendirmesi 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

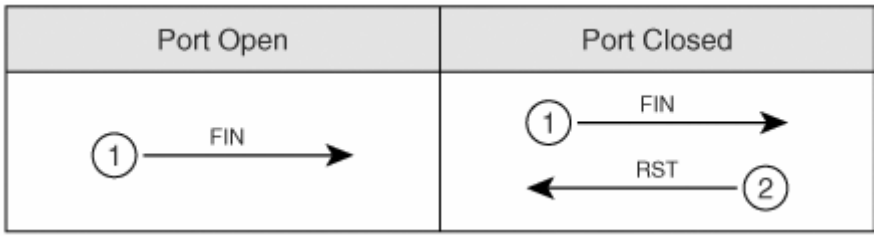

(1) Planning & Preparation
(2) ASSESSMENT
Information Gathering
1
Network Mapping
2
Vulnerability Identification
3
Penetration
4
Gaining Access & Privilege Escalation
5
Enumerating Further
6
Compromising Remote Users/Sites
7
Maintaining Access
8
Covering Tracks
9
Penetration Testing Methodology
(3) Reporting, Clean Up and Destroy Artifacts

Açıkkod Test Araçları



Keşif Süreci

- Pasif Keşif
  - E-posta listeleri, ilan siteleri, netcraft , arama motorları
- Aktif Keşif
  - Samspade, dig/nslookup, whois, nmap, mail başlıkları



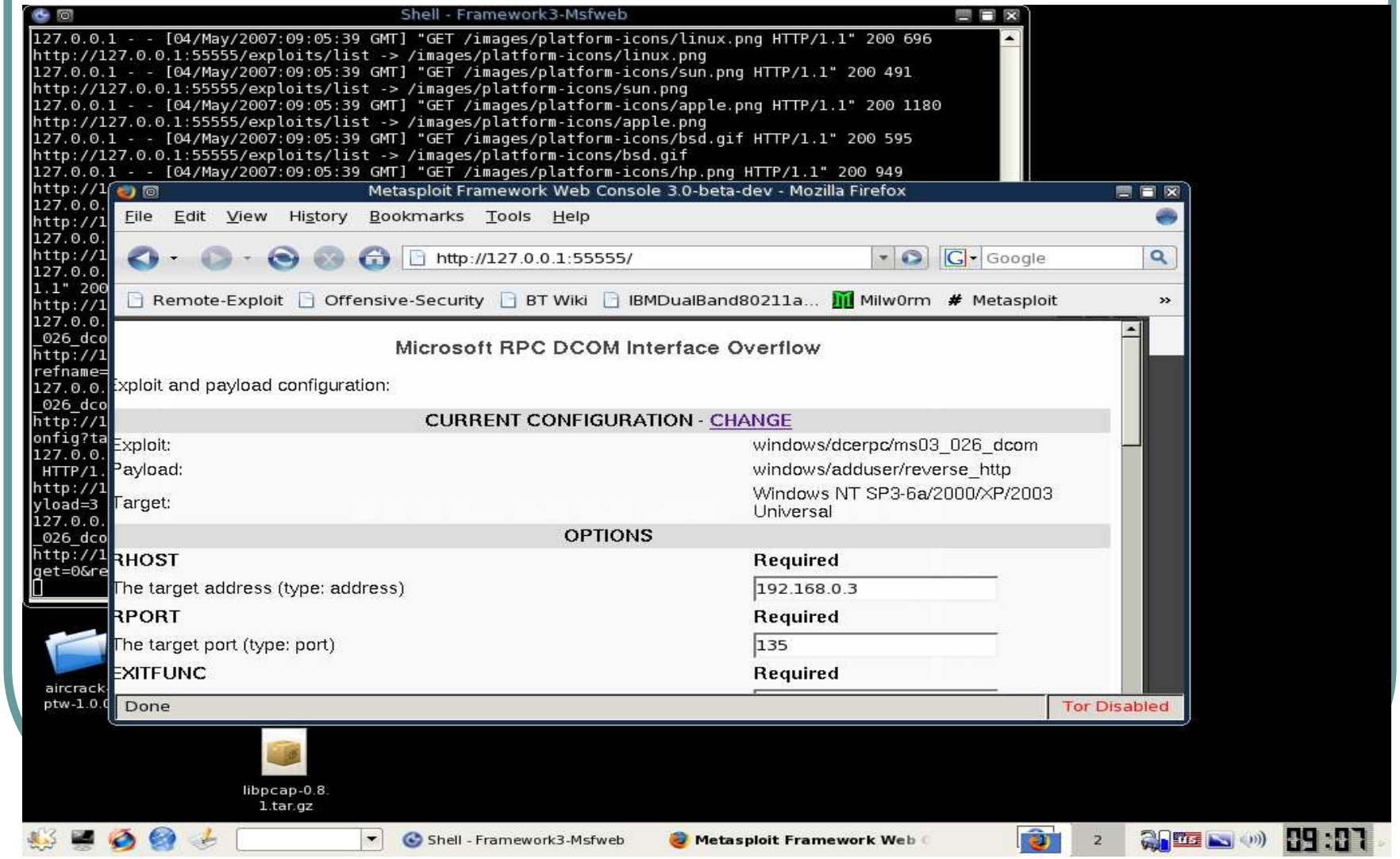
Ağ Haritası Çıkarma

- 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~ acıklık tanıma imzası
- NASL ile zayıflık tanımlama özelliği

Exploit Geliştirme Altyapısı



İçeriden Gelen Saldırılar

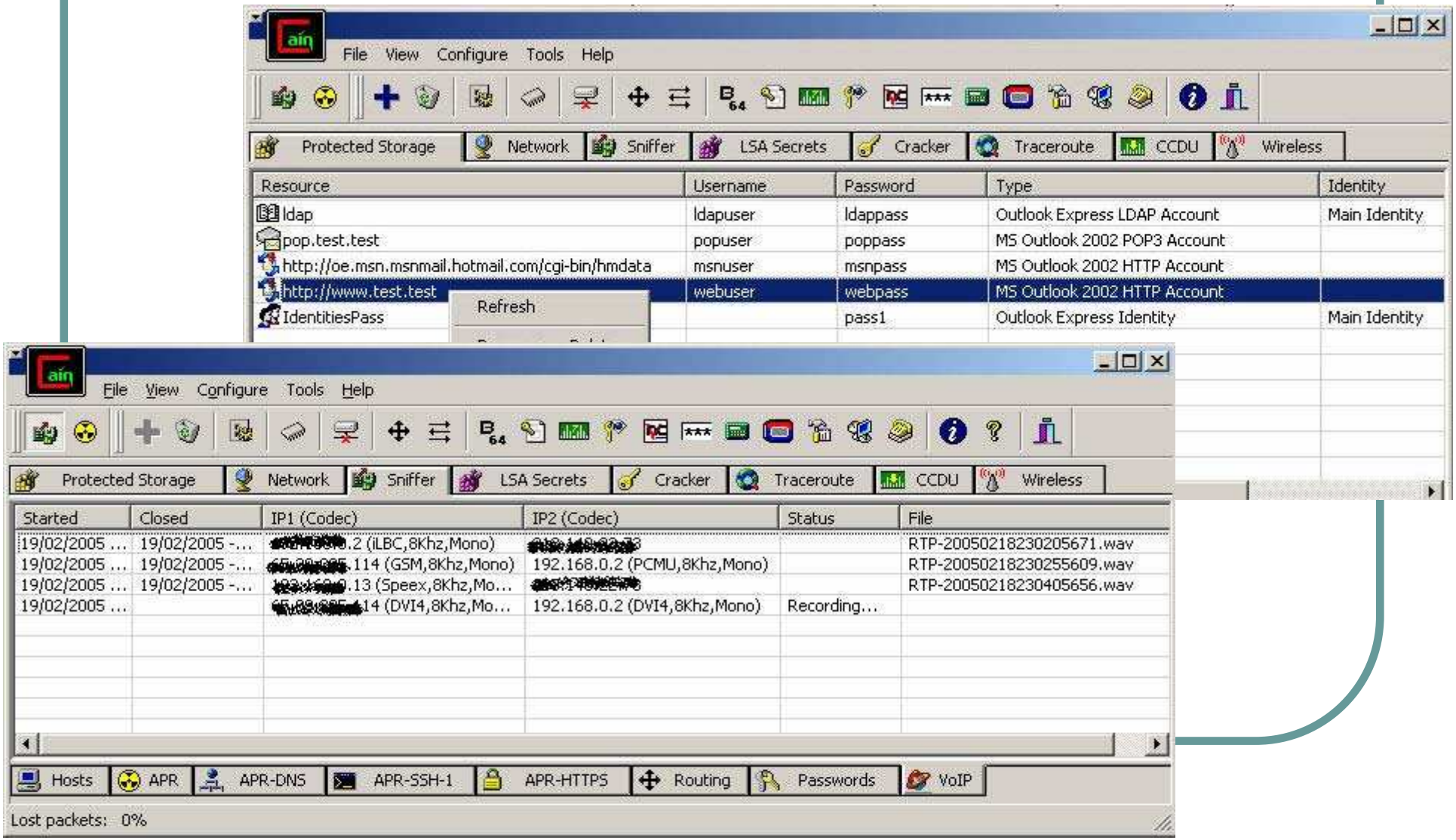
- Yerel Ağ bileşenlerinin zayıflıklarından yararlanılır. (Switch, Hub, Router)
  - IP spoofing, Mac Spoofing, DNS spoofing
  - Ağa izinsiz giren(Wire/less) saldırgan..
  - Şifresiz İletişimleri izleme, müdahele
- Potansiyel suçlu kitlesi!
  - Patronuna kızan çalışan!
  - Meraklı, bilgili bilgisayar kullanıcıları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

LAN Saldırı Araçları..

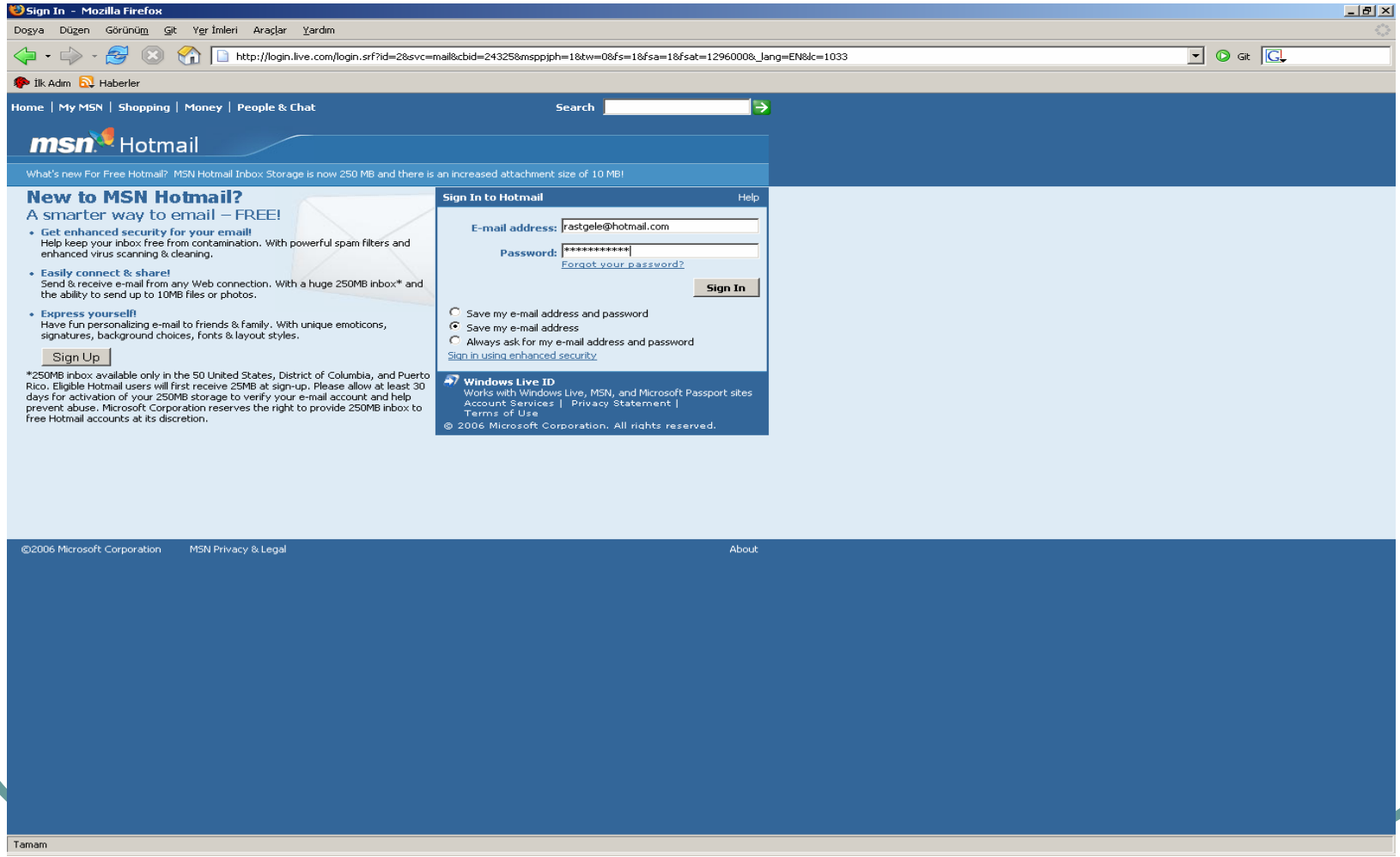
- Trafik Dinleme Araçları: Wireshark, snort, tcpdump
- Şifreli, şifresiz oturumlara müdahele
  - Ettercap

- İsviçre Çakısı: Cain & Abel

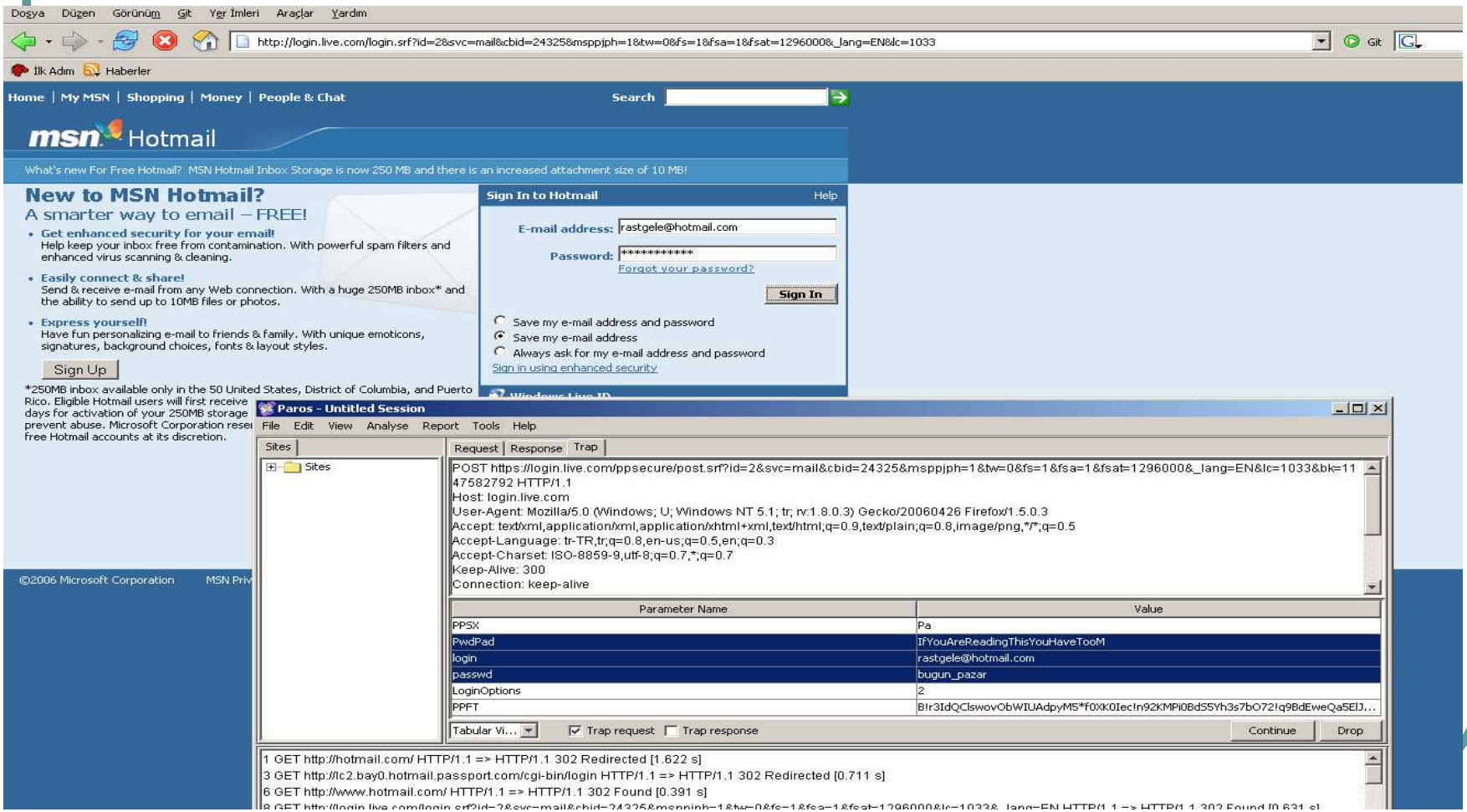
Cain & Abel


File View Configure Tools Help
Protected Storage
Network
Sniffer
LSA Secrets
Cracker
Traceroute
CCDU
Wireless
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
Refresh
Started
Closed
IP1 (Codec)
IP2 (Codec)
Status
File
19/02/2005 ...
19/02/2005 -...
.2 (iLBC,8Khz,Mono)
RTP-20050218230205671.wav
.114 (GSM,8Khz,Mono)
192.168.0.2 (PCMU,8Khz,Mono)
RTP-20050218230255609.wav
.13 (Speex,8Khz,Mo...
RTP-20050218230405656.wav
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%

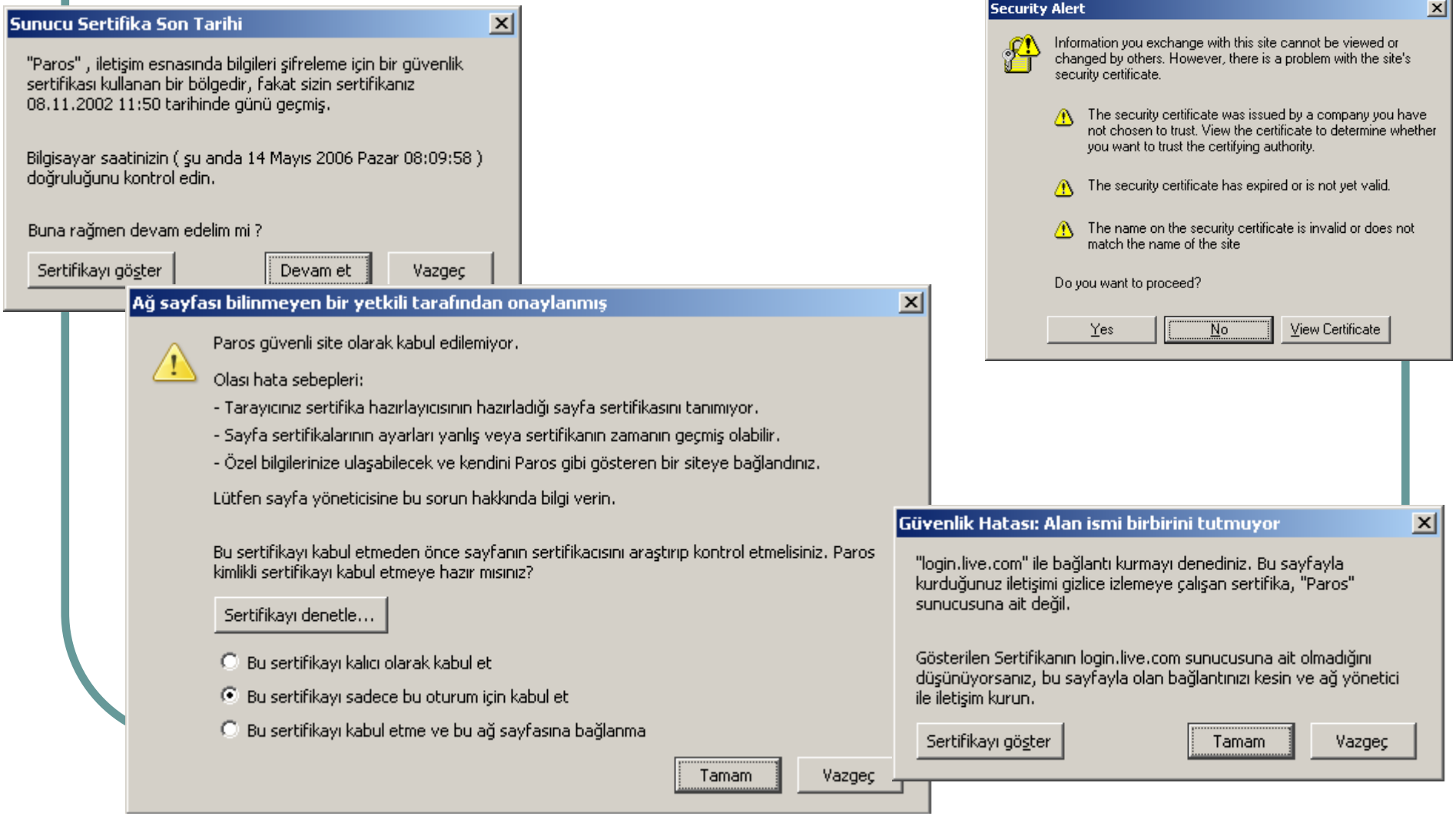
HTTPS Trafigi Degistirme



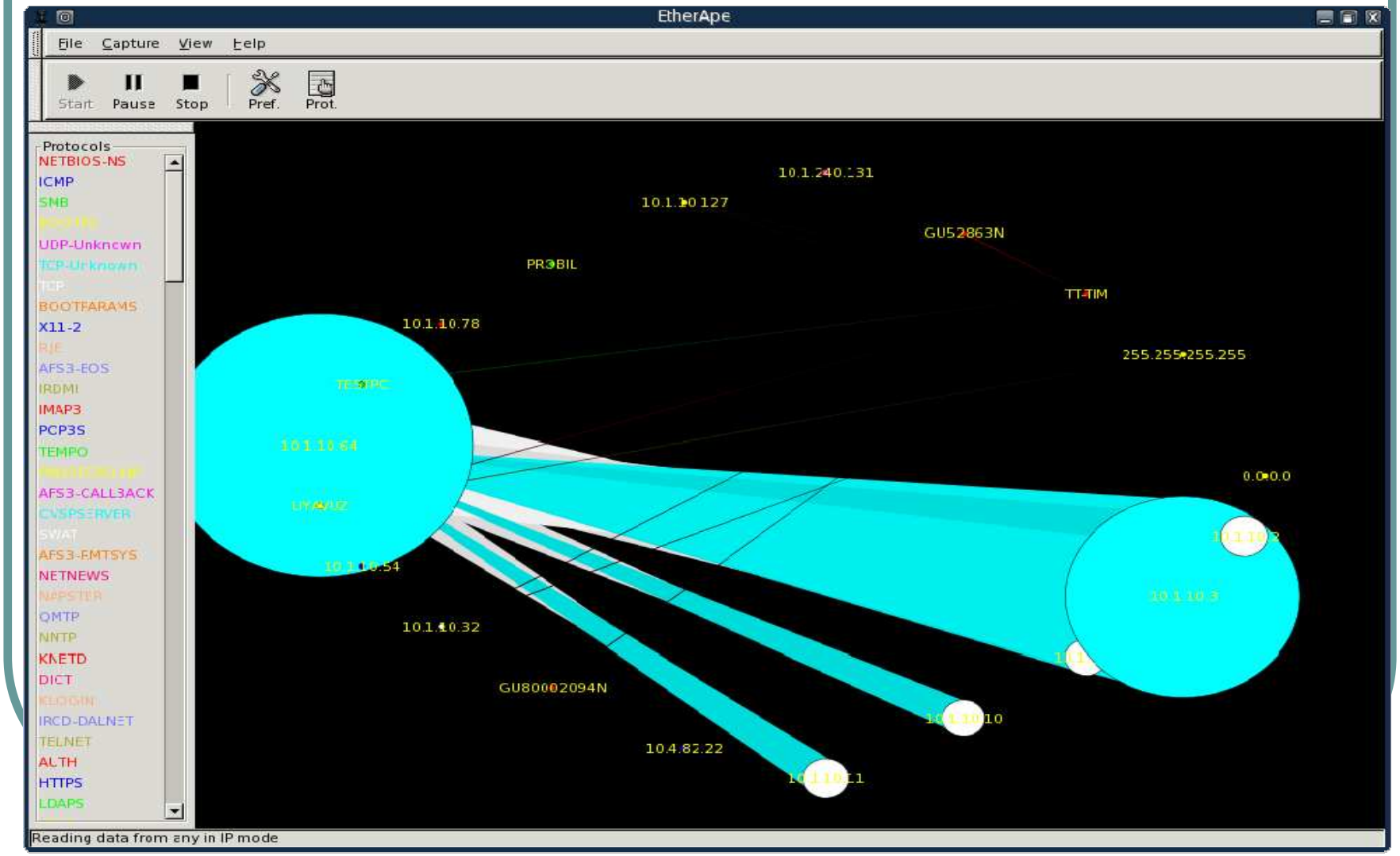
HTTPS Trafigi Degistirme



Firefox/Internet Explorer?



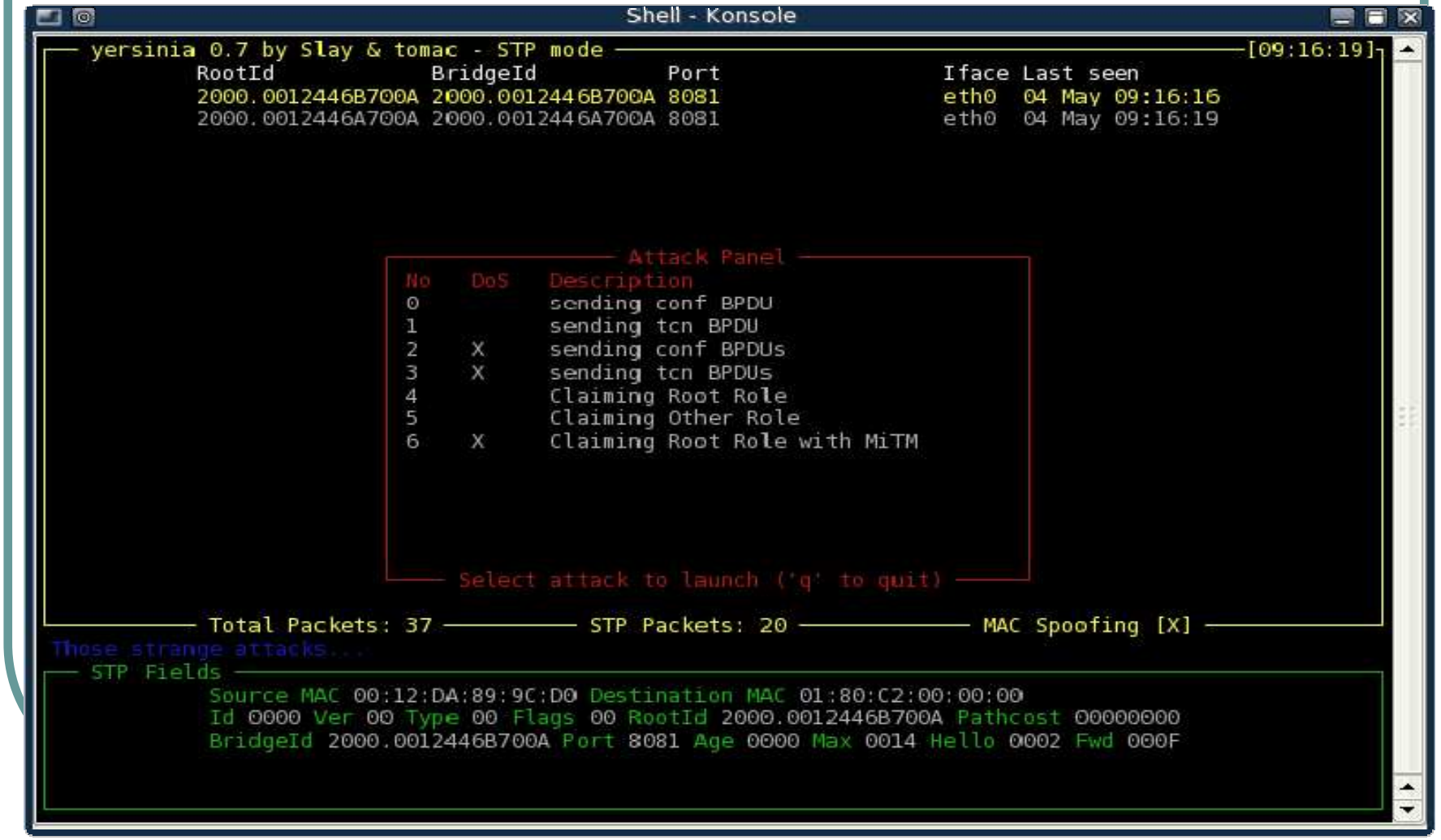
LAN Trafik Analizi



L2 güvenlik testleri-yersinia

- Bilesenleri: 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 Protokolu Güvenliği

- Zone transferi
  - ***$ dig @<dns_sunucu_adresi> -t AXFR huzeyfe.net***
- Ip -> isim çözümleme
  - Passive DNS replication, PTR
- **# dig @ns1.tekrom.com version.bind chaos txt**

;; ANSWER SECTION:

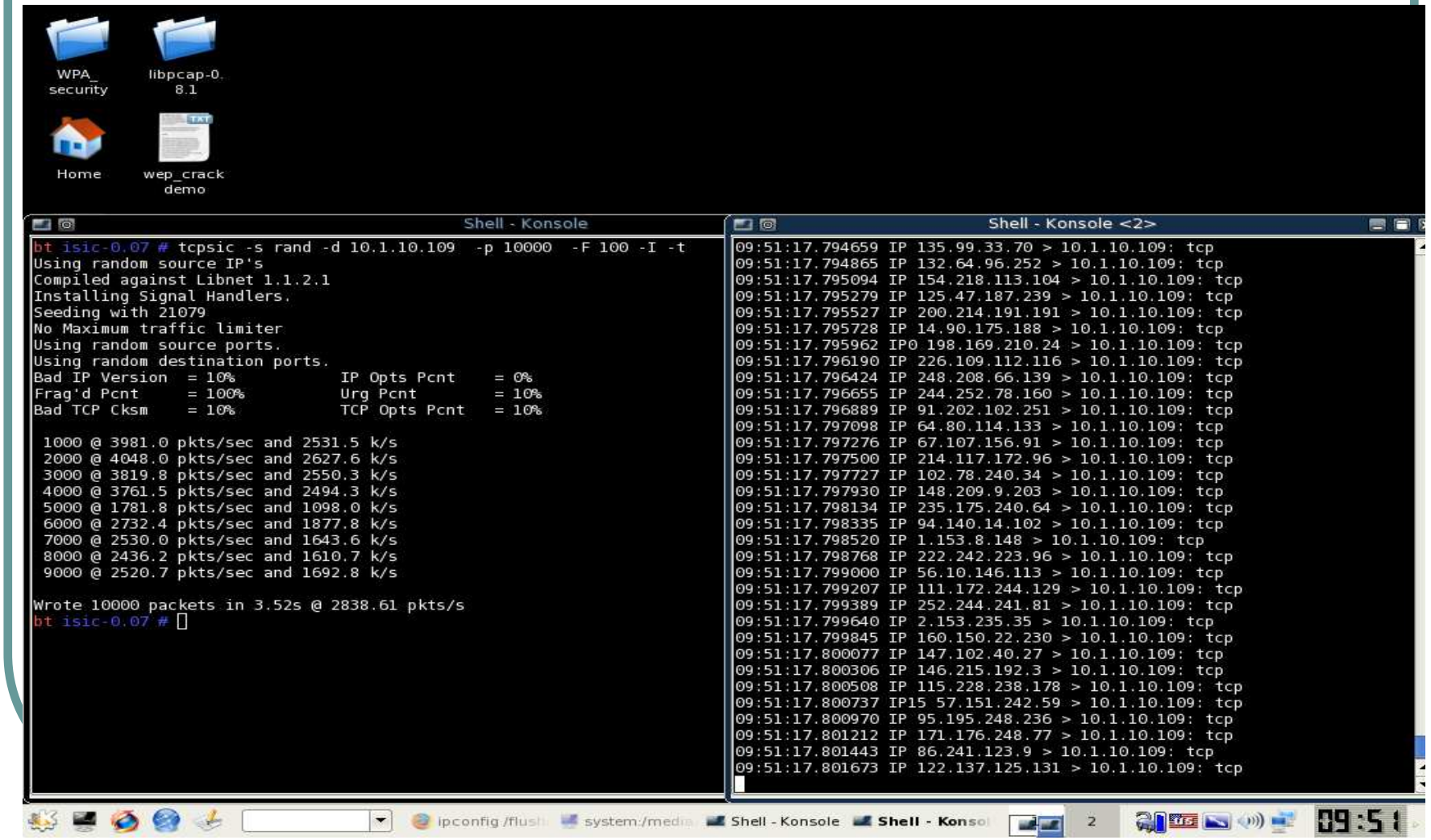
version.bind. 0 CH TXT "9.2.4"

DNS Cache Snooping

- Gercek kayitlarin arasina sahte dns kayitlari eklemek
- Bu sunucuya sorgu yapan tum istemci ve cache dns sunucular zehirlenir...
- Dig +trace www.lifeoverip.net
- Dnsa ile gerçeklenebilir

```
                                        )

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       [illegible]
openbsd.huzeyfe.net.      14400   IN      A       [illegible]
openids.huzeyfe.net.      14400   IN      A       [illegible]
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.[illegible].88
security          14400   IN      A       194.[illegible].88
netsec    14400   IN      A       194.[illegible].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.
```

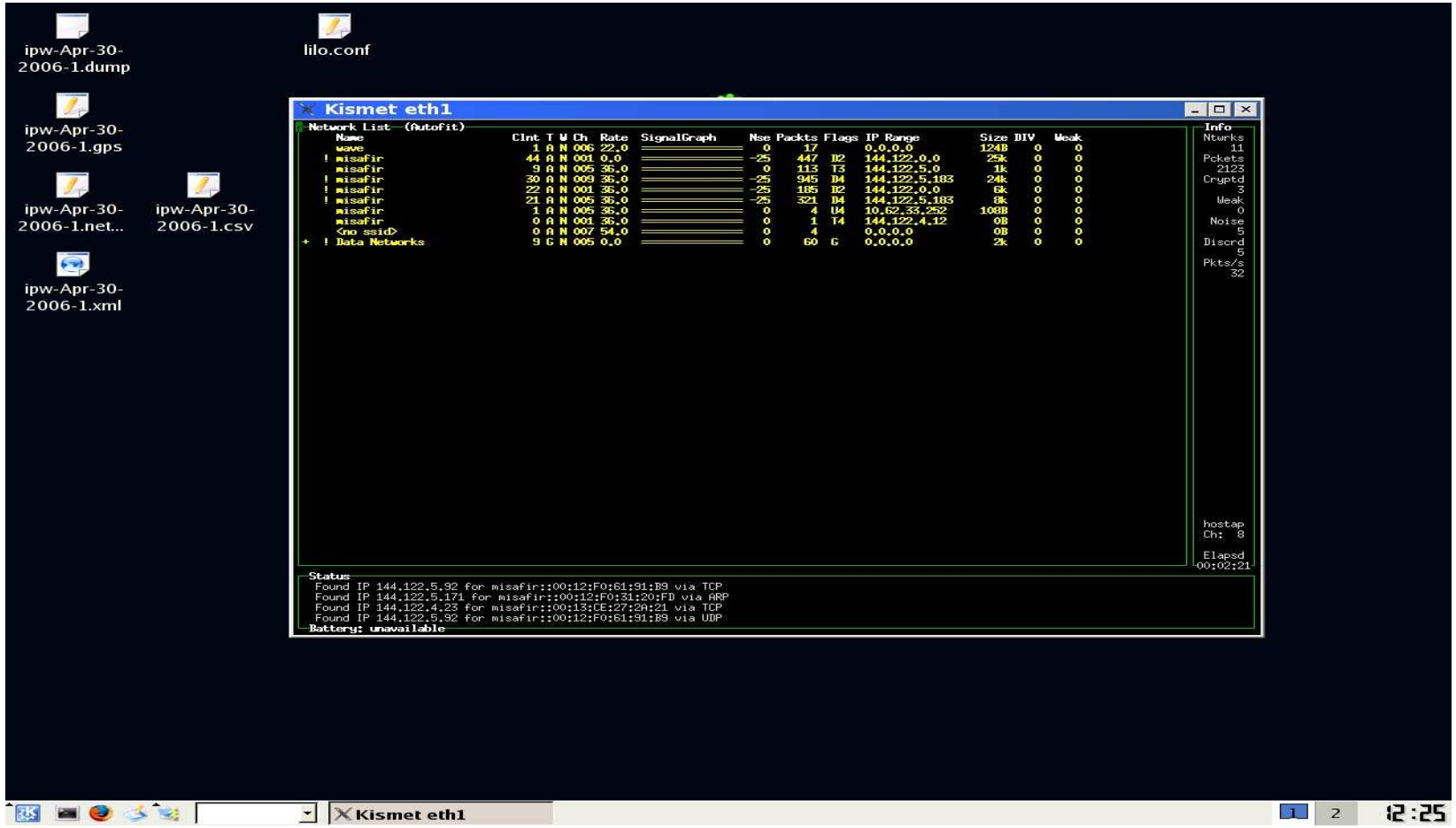
Firewall/IDS Performans Testleri



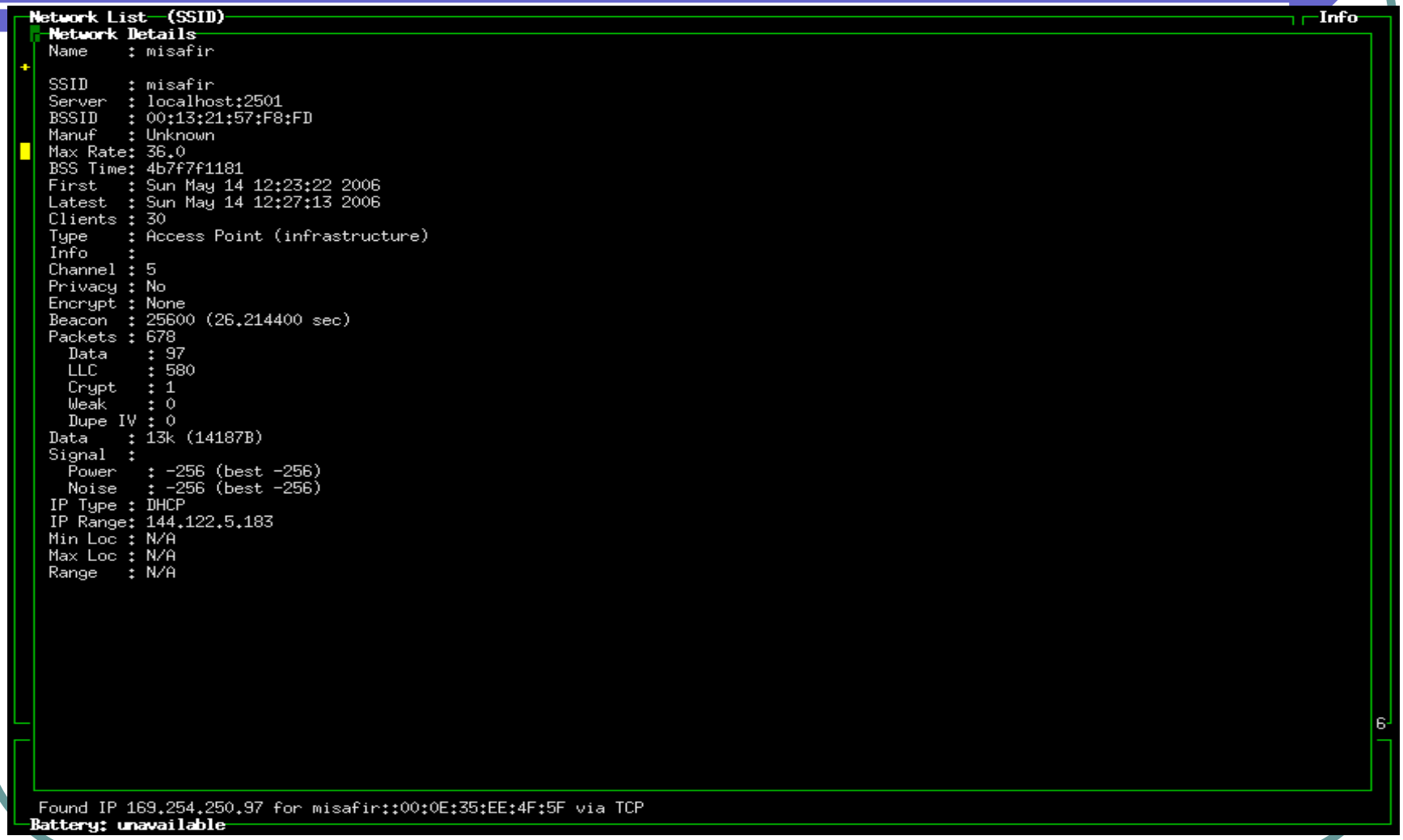
WLAN Güvenliği

- Keşif Araçları
- WEP güvenlik testi
- WPA güvenlik testi
- Sahte AP koumlandirimi
- WLAN Pentest araci

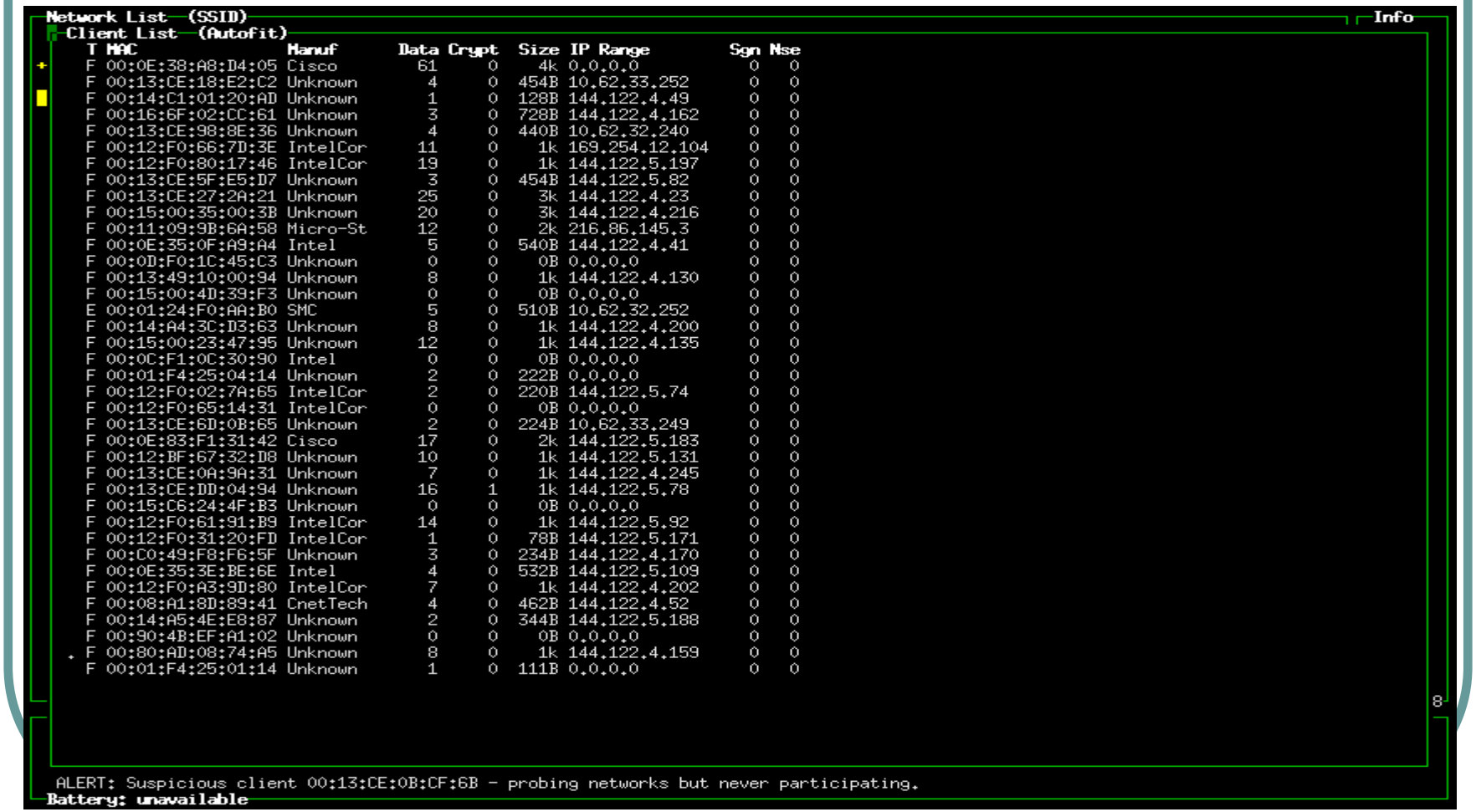
Pasif Keşif: Kismet



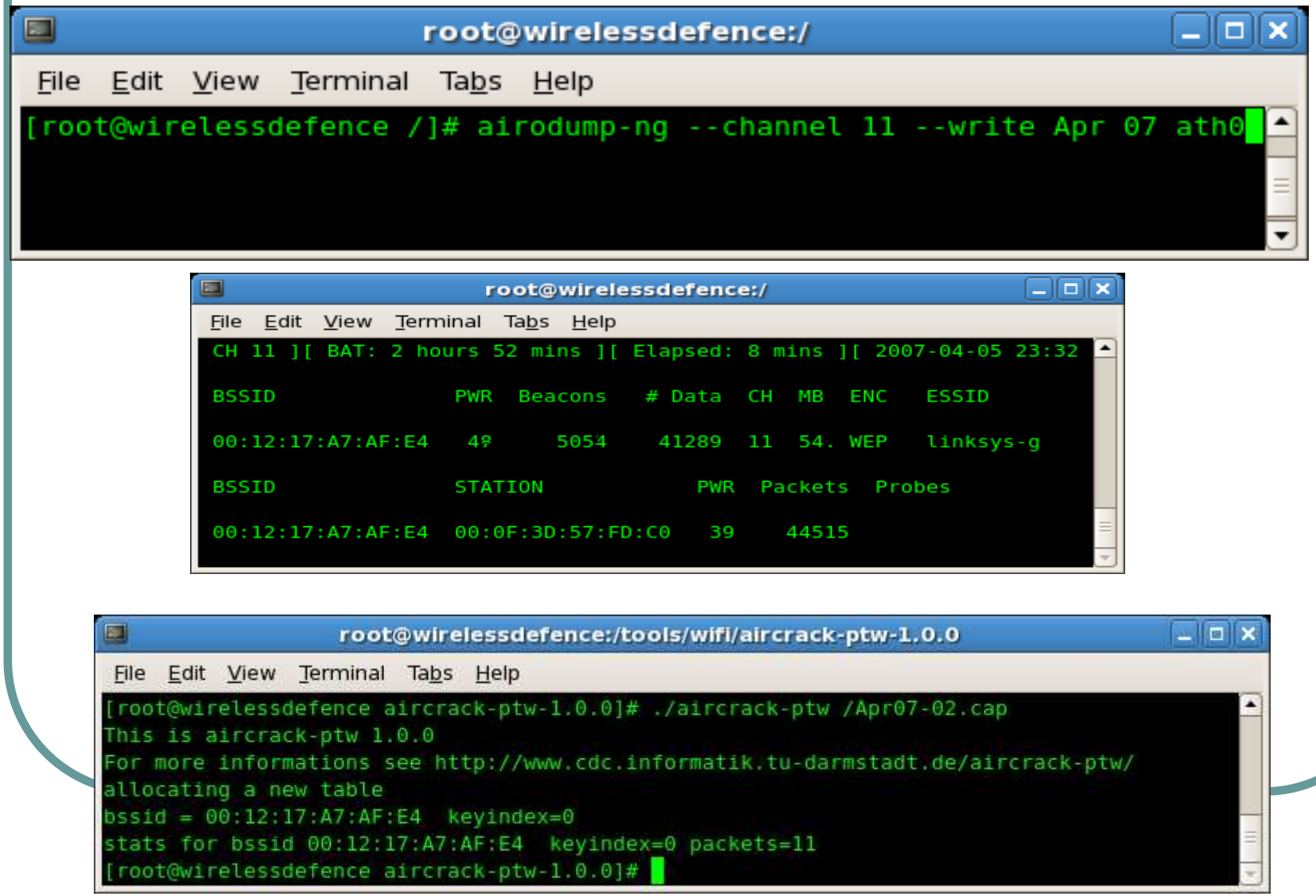
Kismet – AP Kesfi



IP araligini Bulma

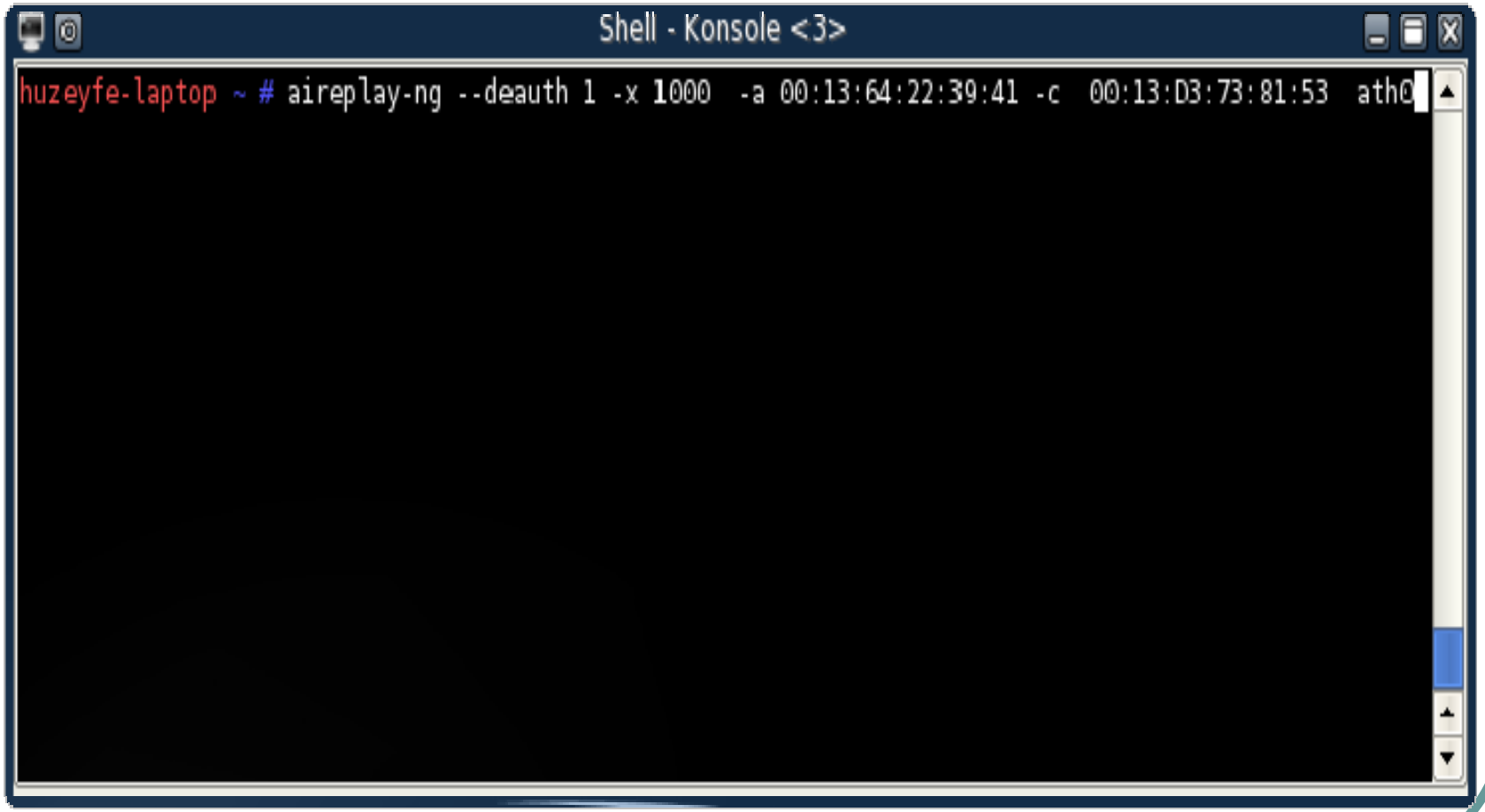


Hızlı WEP Key bulma:aircrack-ptw



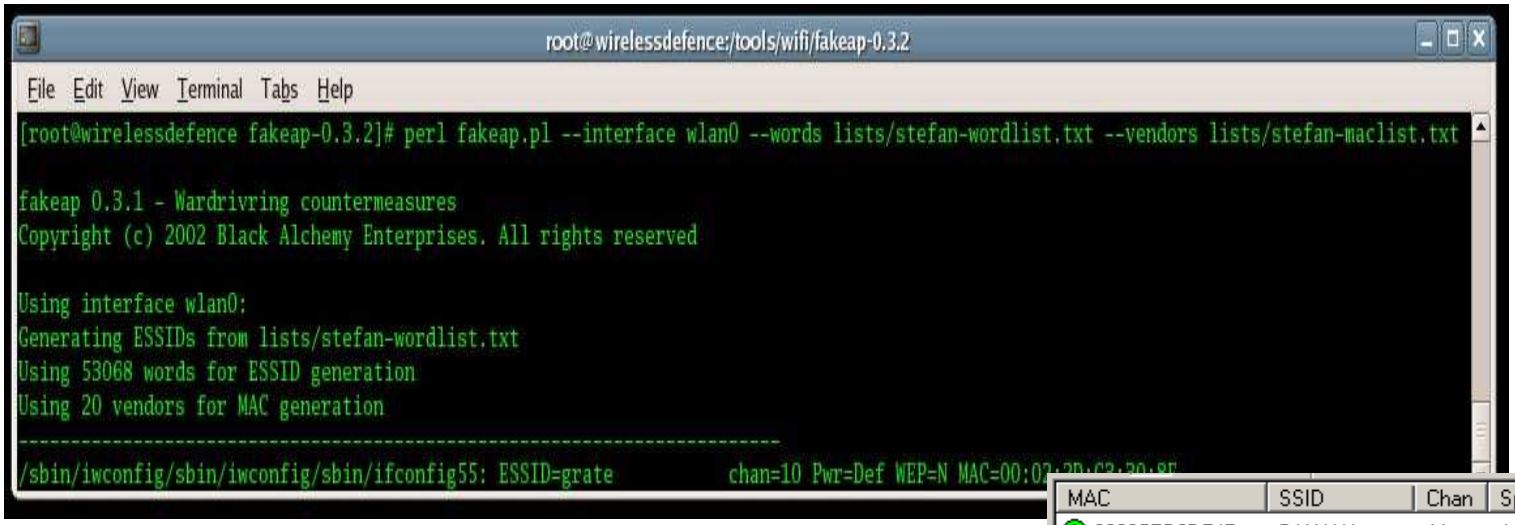
WPA Crack – auth. paketi yakalama

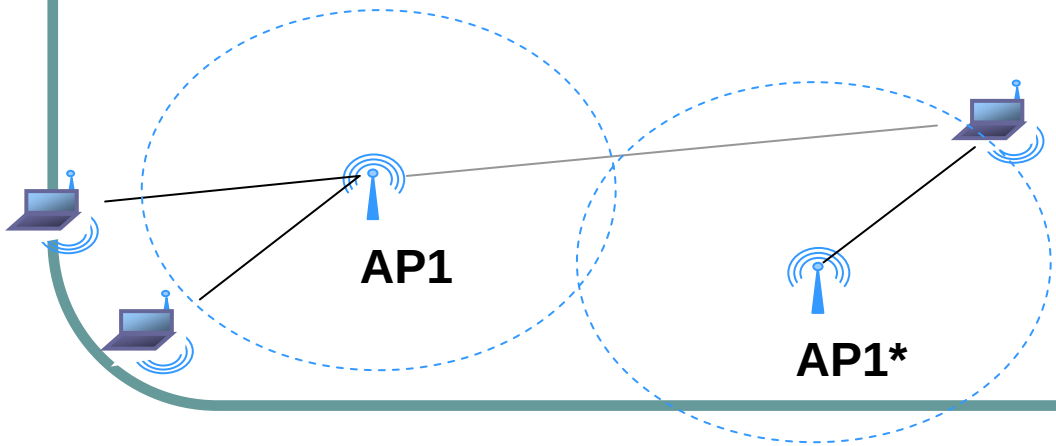
WPA Crack – Ağdan düşürme



WPA Crack – PSK kırma

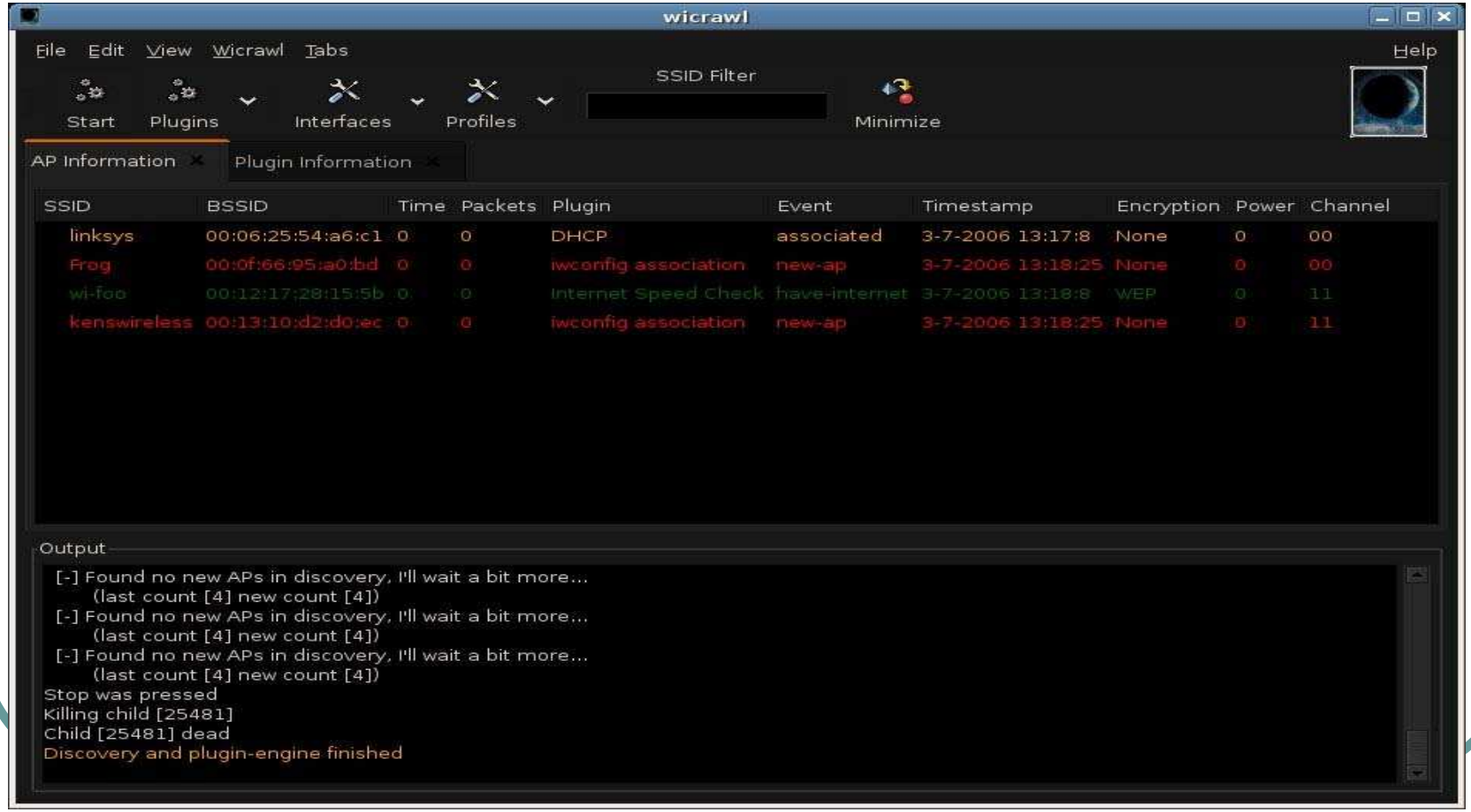
Sahte AP(Erisim Noktalari)





MAC	SSID	Chan	Speed	Type	Enc...
0000CEB8D54F	BANANA	11	11 Mbps	AP	WEP
00000C0B9F8B	BANANA	11	11 Mbps	AP	WEP
00000C72FFC8	BANANA	11	11 Mbps	AP	WEP
00000C8AE489	BANANA	11	11 Mbps	AP	WEP
00000C361C75	BANANA	11	11 Mbps	AP	WEP
00000C1FA804	BANANA	11	11 Mbps	AP	WEP
0000CE022FC4	BANANA	11	11 Mbps	AP	WEP
00000CCB8DD6	BANANA	11	11 Mbps	AP	WEP
0000CE579BE7	BANANA	11	11 Mbps	AP	WEP
00000C5BC03C	BANANA	11	11 Mbps	AP	WEP
00000C76DE04	BANANA	11	11 Mbps	AP	WEP
00000CB07399	BANANA	11	11 Mbps	AP	WEP
0000CE6128F6	BANANA	11	11 Mbps	AP	WEP
00000C37AD95	BANANA	11	11 Mbps	AP	WEP
0000CE11EF14	BANANA	11	11 Mbps	AP	WEP
0000CE9A74CB	BANANA	11	11 Mbps	AP	WEP

Wi-fi Pentest - Wicrawl



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
weplab-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

TEŞEKKÜRLER

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

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