

Computer Network Defence Operational Picture

Security News

BRICKServer from SAGE Inc

US prepares to hack the world
vnunet.com

Biometric passport cracked in 2
hours
Hackers News

Microsoft scrambles to patch security
hole in Windows operating...
Channel NewsAsia

Computer Network Defence

Alert State

	Mozilla	VHCS	Microsoft
Patch	2	2	1



Security Alerts

Latest Threats

- 1 02-07-06 [Backdoor.Prosti](#)
- 2 02-04-06 [W32.Beagle.DN@mm](#)
- 2 02-02-06 [W32.Beagle.DM@mm](#)
- 2 02-02-06 [W32.Beagle.DL@mm](#)
- 2 02-02-06 [W32.Kiman.A](#)

[More...](#)

[Use this feed on your site](#)

Security Vulnerabilities

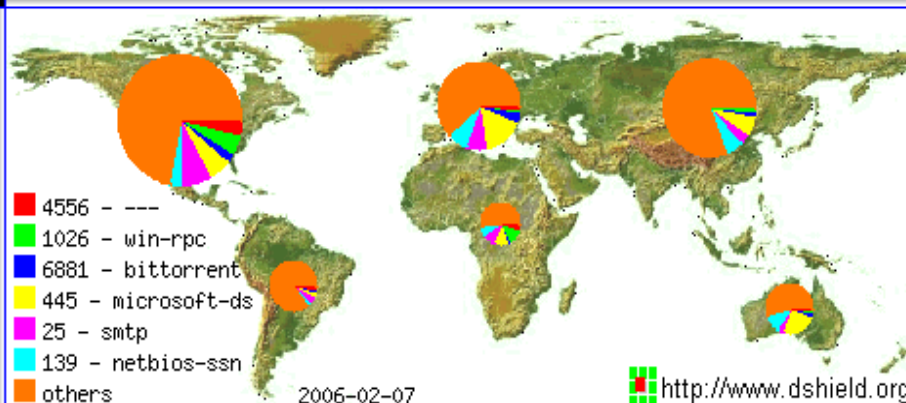
Clever Copy input validation flaw in
'mailarticle.php' Permits SQL
Injection Attacks

cPanel 'mime/handle.html' Input
Validation Bug Permits Cross-Site
Scripting Attacks

Borland Delphi-BCB/Compiler
Integer Overflow May Let Users
Execute Arbitrary Code

CommuniGate Pro LDAP Bug Lets
Remote Users Deny Service

dshield Geographic Port Probe Distribution



Latest Tool Versions

Nmap	31Jan06	4.00
Nessus Client	13Jan06	1.0 RC4
Ethereal	27Dec05	0.10.14
Nessus	12Dec05	3.0.0
Cain & Abel	12Dec05	2.81
Metasploit	21Oct05	2.5
Snort	17Oct05	2.4.3
Kismet	15Aug05	05-08-R1

Latest IDS Signatures

Cisco IPS	03Feb06	S215
Symantec IPS	25Jan06	v39
Proventia	10Jan06	24.27
Intrushield 2.1	05Oct05	2.1.26.2
SecureNetPro	28Feb05	3.9
Manhunt 3.0	09Feb05	v10

Los Angeles	Chicago	New York	GMT/UTC	London	Europe	Baghdad	Tokyo	Sydney	Wellington NZ
09: 10 ⁰⁸	11: 10 ⁰⁸	12: 10 ⁰⁸	17: 10 ⁰⁸	17: 10 ⁰⁸	18: 10 ⁰⁸	20: 10 ⁰⁸	02: 10 ⁰⁸	04: 10 ⁰⁸	06: 10 ⁰⁸

Ag Trafiki Dinleme Ve Yorumlama

Huzeyfe ÖNAL

huzeyfe@enderUNIX.org

EnderUNIX Yazılım Geliştirme Ekibi



Sunum İeriđi

- Paket Kavramı
- Ham trafik, Protokoller ve alıřma yapıları
- Tcpdump paket analizi
- Ethereal ile ađ trafik analizi
- Data Carving
- Yerel Ađlarda Gvenlik sorunsalı
- řifrelenmiř trafik Gvenli mi?
- zmler..

Sniffing for what?

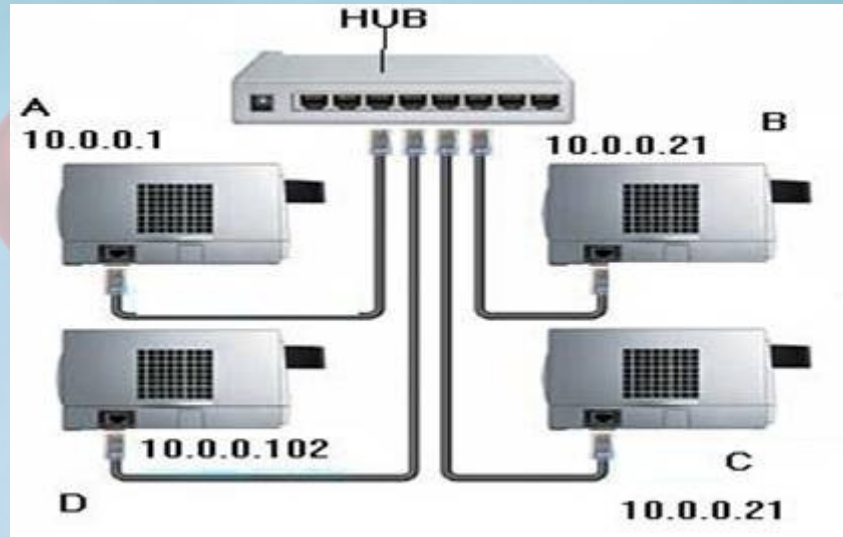
- Good/Admins = “Protocol Analysis”
- Bad/Hackers = “Sniffing The Wire”
- Developers = “Is My Application Working

Paket Kavramı..

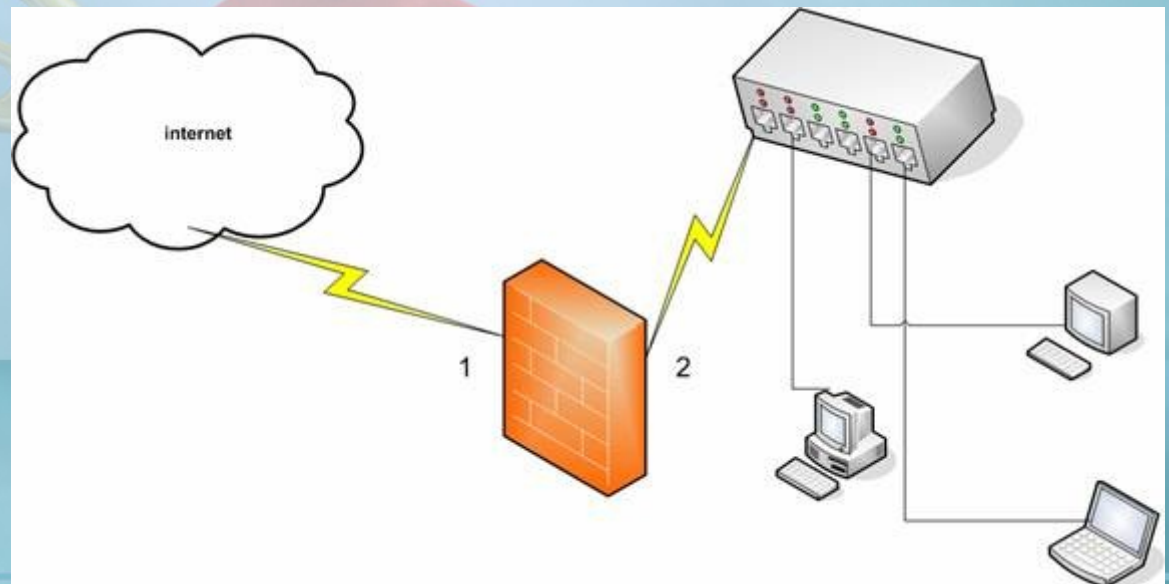
- İletişim == paket (?)
- Ne işe yarar
 - Bilinmeyen Protokol Analizi
 - Ağ trafiği başarımları
 - Anormal trafik gözleme
 - Firewall/IDS/IPS altyapısı..
- TCP, UDP Paketleri
- Protokoller
 - SMTP, FTP, P2P trafiği nasıl ayırt edilir
 - Linux L7-filter projesi

L2 İletişim Ortamları

- HUB



- Switch



Ham Trafik

- Tcpdump çıktısı – 68 byte

16:21:24.174180 192.168.60.3.34720 >
10.10.10.3.3389: S
2354677536:2354677536(0) win 5840
<mss 1460,sackOK,timestamp 25027249
0,nop,wscale 0> (DF)

Tcpdump analizi

- 16:21:24.174180 Timestamp
- 192.168.60.3 Source IP address
- 34720 Source port
- 10.10.10.3 Destination IP address
- 3389 Destination port
- S TCP SYN flag is set
- 2354677536 TCP initial sequence number (ISN)
- ...

Ethereal ile trafik Analizi

eth1: Capturing - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
23	50.078265	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
24	50.081516	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
25	50.084511	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
26	50.087982	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
27	50.091351	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
28	50.094766	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
29	50.098247	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
30	54.316460	Intel_d8:df:c9	Broadcast	ARP	Who has 192.168.1.1? Tel
31	54.320625	USRoboti_e8:aa:7c	Intel_d8:df:c9	ARP	192.168.1.1 is at 00:c0:4
32	54.320638	192.168.1.2	212.175.212.2	DNS	Standard query A google.c
33	59.315736	192.168.1.2	212.175.212.2	DNS	Standard query A google.c
34	59.347324	212.175.212.2	192.168.1.2	DNS	Standard query response A 64.233.167.99 A 64.233.187.99 A 72.14

Ethereal: Capture from eth

Captured Packets

Total	% of total
50	
SCTP	0.0%
TCP	0.0%
UDP	88.0%
ICMP	4.0%
ARP	8.0%
OSPF	0.0%
GRE	0.0%
NetBIOS	0.0%
IPX	0.0%
VINES	0.0%
Other	0.0%

Running 00:01:39 [Stop]

Frame 1 (320 bytes on wire, 320 bytes captured)

Ethernet II, Src: USRoboti_e8:aa:7c (00:c0:49:e8:aa:7c), Dst: 01:00:5e:7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 239.255.255.250 (239.255.255.250)

User Data

Hypertext

Shell - Konsole

```
root@slax:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0E:35:D8:DF:C9
          inet addr:1.1.1.2  Bcast:1.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::20e:35ff:fed8:dfc9/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:137 errors:0 dropped:69 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6880 (6.7 Kb)  TX bytes:568 (568.0 b)
          Interrupt:7  Base address:0x2000  Memory:fcffe000-fcffe000

root@slax:~# ifconfig eth1 192.168.1.2
root@slax:~# route add default gw 192.168.1.1
root@slax:~# ping google.com
PING google.com (64.233.167.99) 56(84) bytes of data:
64 bytes from 64.233.167.99: icmp_seq=1 ttl=242 time=198 ms
```

eth1: <live capture in progress> File: /tmp/etherXXXXZfviPJ 14 KB P: 50 D: 50 M: 0

ARP Analizi

The screenshot displays a network analysis setup. The top window is Wireshark, capturing traffic on the eth1 interface. It shows four ARP requests in the packet list. The bottom section of Wireshark shows the details of the first frame, which is an ARP request from Intel_d8:df:c9 to the broadcast address ff:ff:ff:ff:ff:ff.

Below Wireshark, there are two terminal windows. The left terminal, titled 'Shell - Konsole', shows the execution of the following commands:

```
root@slax:~# arp -an
? (192.168.1.1) at 00:C0:49:E8:AA:7C [ether] on eth1
root@slax:~# arp -d 192.168.1.1
root@slax:~# arp -an
? (192.168.1.1) at <incomplete> on eth1
root@slax:~# arp -an
? (192.168.1.1) at 00:C0:49:E8:AA:7C [ether] on eth1
root@slax:~#
```

The right terminal, also titled 'Shell - Konsole', shows the execution of a ping command and its statistics:

```
root@slax:~# ping google.com
PING google.com (72.14.207.99) 56(8
-) bytes of data:
. 4 bytes from 72.14.207.99: icmp_se
=1 ttl=241 time=182 ms

-- google.com ping statistics --
. packets transmitted, 1 received,
% packet loss, time 0ms
tt min/avg/max/mdev = 182.029/182.
29/182.029/0.000 ms
root@slax:~#
```

On the far right, a small window titled ': Capture from eth' shows a bar chart of packet statistics. The chart has a single bar for '4' packets, representing 100.0% of the total. Below the chart, there is a 'Stop' button and a timestamp '0:01:04'.

The bottom status bar of the application shows 'eth1: <live capture in progress> File: /tmp/etherXXXXn4VV3g 256 Bytes' and 'P: 4 D: 4 M: 0'. The system tray at the bottom right shows the time as '06:40'.

Ethereal Paket detaylari

eth1: Capturing - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	64.90.164.206	TCP	41244 > http [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 TSV=2074
2	0.168823	64.90.164.206	192.168.1.2	TCP	http > 41244 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS
3	0.168850	192.168.1.2	64.90.164.206	TCP	41244 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=207615 TSER=
4	9.023631	192.168.1.2	64.90.164.206	HTTP	Continuation or non-HTTP traffic
5	9.246999	64.90.164.206	192.168.1.2	HTTP	Continuation or non-HTTP traffic
6	9.247024	192.168.1.2	64.90.164.206	TCP	41244 > http [ACK] Seq=34 Ack=1441 Win=8720 Len=0 TSV=216695 TS
7	9.273554	64.90.164.206	192.168.1.2	HTTP	Continuation or non-HTTP traffic
8	9.273566	192.168.1.2	64.90.164.206	TCP	41244 > http [ACK] Seq=34 Ack=2881 Win=11600 Len=0 TSV=216721 "
9	9.296291	64.90.164.206	192.168.1.2	HTTP	Continuation or non-HTTP traffic
10	9.296301	192.168.1.2	64.90.164.206	TCP	41244 > http [ACK] Seq=34 Ack=4097 Win=14480 Len=0 TSV=216744 "
11	9.323576	64.90.164.206	192.168.1.2	HTTP	Continuation or non-HTTP traffic
12	9.323586	192.168.1.2	64.90.164.206	TCP	41244 > http [ACK] Seq=34 Ack=5537 Win=17360 Len=0 TSV=216771 "

Frame 3 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Intel_d8:df:c9 (00:0e:35:d8:df:c9), Dst: USRoboti_e8:aa:7c (00:c0:49:e8:aa:7c)
Internet Protocol Src: 192.168.1.2 (192.168.1.2), Dst: 64.90.164.206 (64.90.164.206)
Shell - Konsole (80), Seq: 1, Ack: 1, Len: 0

Shell

```
root@slax:~# telnet www.enderunix.org 80
Trying 64.90.164.206...
Connected to www.enderunix.org.
Escape character is '^]'.
-----
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; chars
et=iso-8859-9" />
<title>EnderUNIX Yazilim Gelistirme Takimi @ TR </title>
<link href="style.css" rel="stylesheet" type="text/css" /
>
</head>
<body>
<div align="center">
<div align="center">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
```

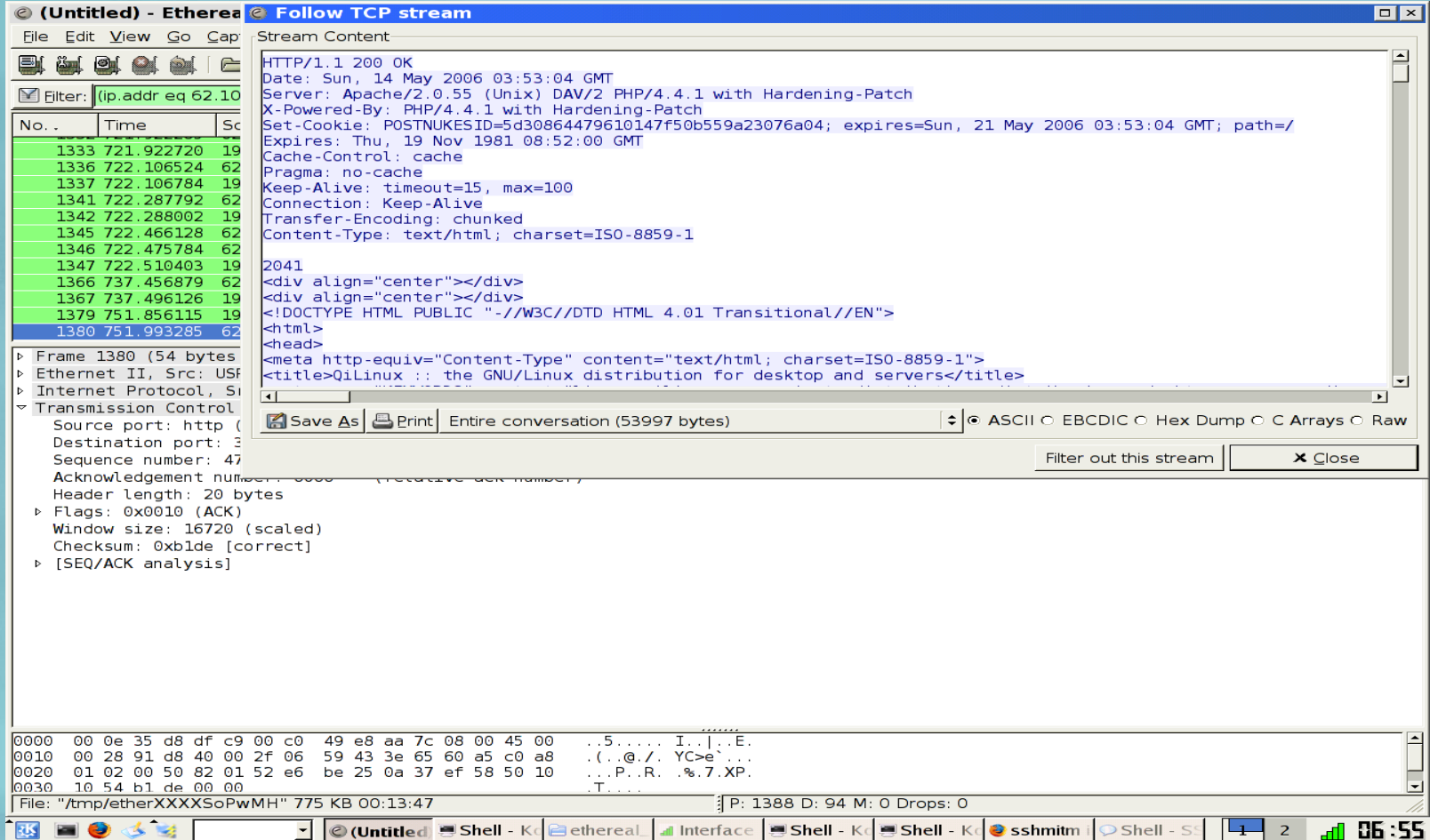
Ethereal: Capture from eth1

Captured Packets	Total	% of total
SCTP	0	0.0%
TCP	31	100.0%
UDP	0	0.0%
ICMP	0	0.0%
ARP	0	0.0%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	0	0.0%

Running 00:01:40
Stop

eth1: <live capture in progress> File: /tmp/etherXXXXSoPwMH 19 KB P: 31 D: 31 M: 0

HTTP oturum Detayı



Normal- Anormal Trafik..

Sguil [sguil] - SGUIL-0.3.0

File Query Reports Database Sound: Off 2003-12-23 15:43:41 GMT

RealTime Events Escalated Events Event Query 1

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	bourque	1.13375	2003-12-23 11:53:23	68.86.32.20	3575	68.84.6.72	80	6	WEB-IIS _mem_bin access
RT	1	bourque	1.13401	2003-12-23 13:17:21	217.204.187.168	3125	68.84.6.72	1434	17	MS-SQL Worm propagation attempt
RT	1	bourque	1.14656	2003-12-23 14:58:16	172.165.197.90	1720	68.84.6.72	1434	17	MS-SQL Worm propagation attempt
RT	1	bourque	1.14725	2003-12-23 15:33:13	220.111.108.28	1340	68.84.6.72	1434	17	MS-SQL Worm propagation attempt

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	52	bourque	1.12167	2003-12-18 16:22:27	68.84.6.72	1131	204.152.184.73	21	6	POLICY FTP anonymous login attempt
RT	27	bourque	1.12171	2003-12-18 16:41:33	68.84.6.72	32845	66.193.208.66	21	6	POLICY FTP anonymous (ftp) login attempt
RT	2	bourque	1.12172	2003-12-18 16:42:04	66.193.208.66	20	68.84.6.72	32849	6	snort_decoder: Truncated Tcp Options
RT	1332	bourque	1.13425	2003-12-23 14:40:24	68.84.6.72	1114	68.48.0.5	53	17	LOCAL Large UDP DNS packet

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	bourque	1.13181	2003-12-23 01:43:46	66.192.0.70	47889	68.84.6.72	80	6	spp_stream4: NMAP Fingerprint Stateful Detection
RT	2	bourque	1.13183	2003-12-23 01:43:46	66.192.0.70	47892	68.84.6.72	81	6	spp_stream4: NMAP XMAS Stealth Scan
RT	1	bourque	1.13184	2003-12-23 01:43:48	66.192.0.70	47887	68.84.6.72	80	6	spp_stream4: NULL Stealth Scan
RT	1	bourque	1.13185	2003-12-23 01:43:48	66.192.0.70	47888	68.84.6.72	80	6	spp_stream4: Stealth Activity Detected

Src IP: 68.84.6.72
Src Name: pcp02347462pcs.manass01.va.comcast.net
Dst IP: 68.48.0.5
Dst Name: ns01.rtrchrd01.md.comcast.net

☒ Reverse DNS Whois Query: ☒ None ☐ Src IP ☐ Dst IP

☒ Show Packet Data ☒ Show Rule www.snort.org

alert udp any any -> any 53 (msg:"LOCAL Large UDP DNS packet"); dsize > 256; classtype:un

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL
UDP	68.84.6.72	68.48.0.5	4	5	0	66	53210	0	0	63

UDP	Port	Port	Length	ChkSum
	1114	53	46	9824

DATA

C7 F5 01 00 00 01 00 0C 00 00 00 00 03 77 77 77
05 79 61 68 6F 6F 06 61 6B 61 64 6E 73 03 6E 65yahoo.akadns.ne
74 00 00 01 00 01t.....



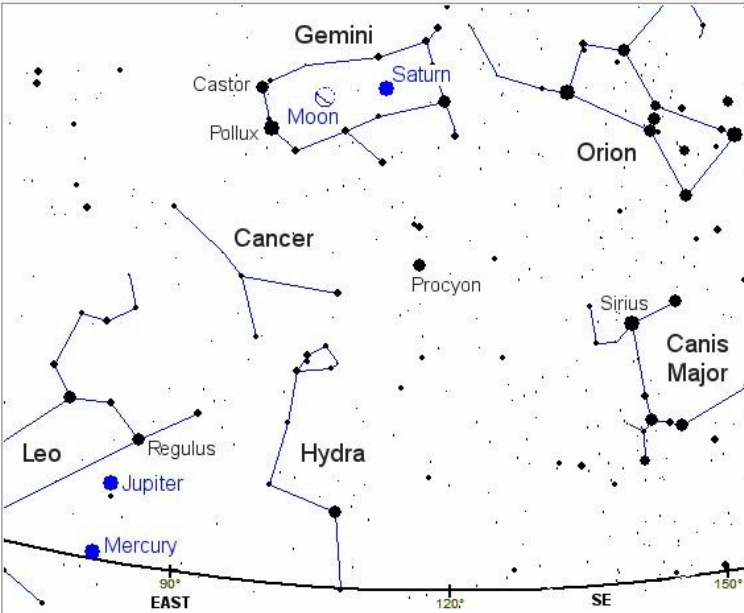
System Messages User Messages

[2003-12-23 14:53:12] bourque: /snort_data 14%
[2003-12-23 15:23:13] bourque: /snort_data 14%

Data Carving...

- Ham veriden orijinal veri elde etme yöntemi
- Örnek;
- **#tcpdump -s9000 host www.enderunix.org -w enderunix**
- arkasından wget ile EnderUNIX altından bir gif dosyası indiriyoruz ve chaosreader ile enderunix dosyasına kaydettiğimiz trafiği okutuyoruz, sonuç?
- **\$perl chaosreader0.94 enderunix**

ChaosReader

7.	Sun Nov 16 20:38:51 2003	192.168.1.3:1371 <-> 192.77.84.99:80	
8.	Sun Nov 16 20:38:51 2003	192.168.1.3:1372 <-> 192.77.84.99:80	
9.	Sun Nov 16 20:38:51 2003	192.168.1.3:1373 <-> 192.77.84.99:80	

Driftnet

The screenshot displays the Driftnet application interface, which is divided into several panels. The top-left panel shows a Google logo with a penguin and a red devil character. Below it, a table lists network traffic data:

IP	Port	Source	Destination
166	437	033846	192.168.1.2
167	437	249190	64.233.183.104
168	437	250581	64.233.183.104
169	437	283191	64.233.183.104
170	437	283208	192.168.1.2
171	437	289048	64.233.183.104
172	437	289080	192.168.1.2
173	437	300346	192.168.1.2
174	437	540939	64.233.183.104

The top-right panel, titled "Shell - Driftnet", contains text about the program's adjunct mode and copyright information:

Adjunct mode is designed to be used by other programs which want to use driftnet to gather images from the network. With the -m option, driftnet will silently drop images if more than the specified number of images are saved in its temporary directory. It is assumed that some other process is collecting and deleting the image files.

driftnet, copyright (c) 2001-2 Chris Lightfoot <chris@ex-parrot.com>
home page: <http://www.ex-parrot.com/~chris/driftnet/>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

The bottom-left panel shows a terminal window with the following output:

```
root@slax:~# telnet www.enderunix.org
Trying 64.90.164.206...
Connected to www.enderunix.org.
Escape character is '^]'.
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-9" />
<title>EnderUNIX Yazilim Gelistirme T...
<link href="style.css" rel="stylesheet" />
</head>
<body>
<div align="center">
<div align="center">
<table width="100%" border="0" cell
```

The bottom-right panel shows a Mozilla Firefox browser window displaying the Google homepage. The address bar shows <http://www.google.com/bdd>. The page content includes the Google logo, a search bar, and the text "Search the entire web from the [Google home page!](#)".

The taskbar at the bottom shows the following applications: eth1: C:, Shell, ethereal, Interface, Shell, Shell, Shell, <Bsd>, X driftnet, and a system tray with a clock showing 06:48.

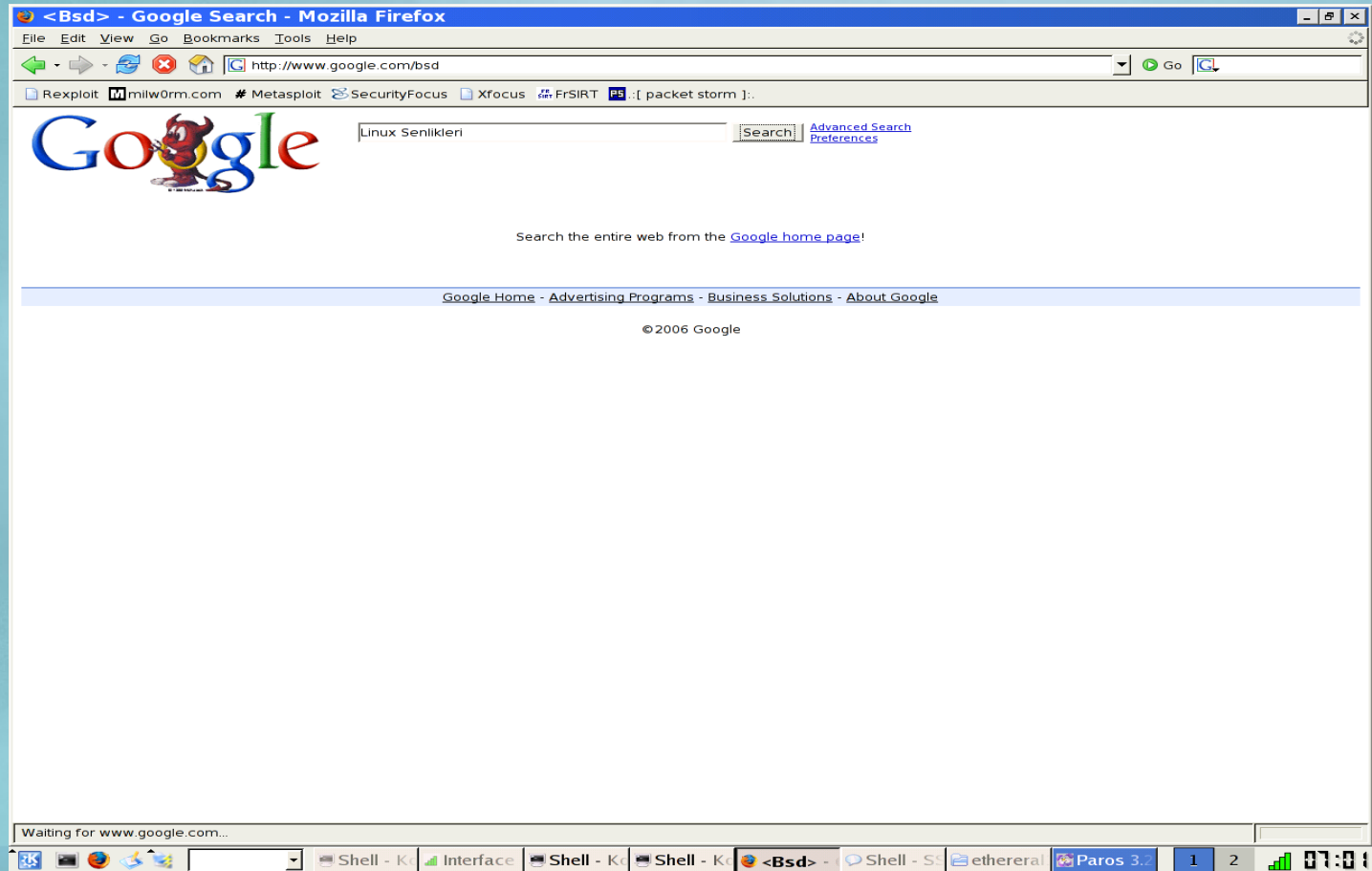
Ağ Performans ölçümü

- Firewall, IDS gibi cihazların trafik kapasitesi
- 1GBps, 150Mbs gibi sayılar ne ifade ediyor?
- Iperf
 - TCP/UDP kullanarak ağ performansı ölçümü
- Bpfstat
 - Drop edilen paket sayısı

Trafik dinleme ile Gerçekleştirilen Saldirilar

- Kandırmaca(Spoofing) Saldırıları
 - MAC, IP, DNS vs..
- Araya Girme,
- Trafik değiştirme, yönlendirme
- Sistem yorma, DOS vs
- **Kötü Durum Senaryosu!!**

Araya Girme Uygulaması-1



Araya Girme Uygulamasi-2

The screenshot shows a web proxy application with a menu bar (File, Edit, View, Analyse, Report, Tools, Help) and a 'Sites' list on the left containing three entries: http://ftp-mozilla.netscape.com, http://google.com, and http://www.google.com. The main window is divided into three tabs: 'Request', 'Response', and 'Trap'. The 'Request' tab is active, displaying the following details:

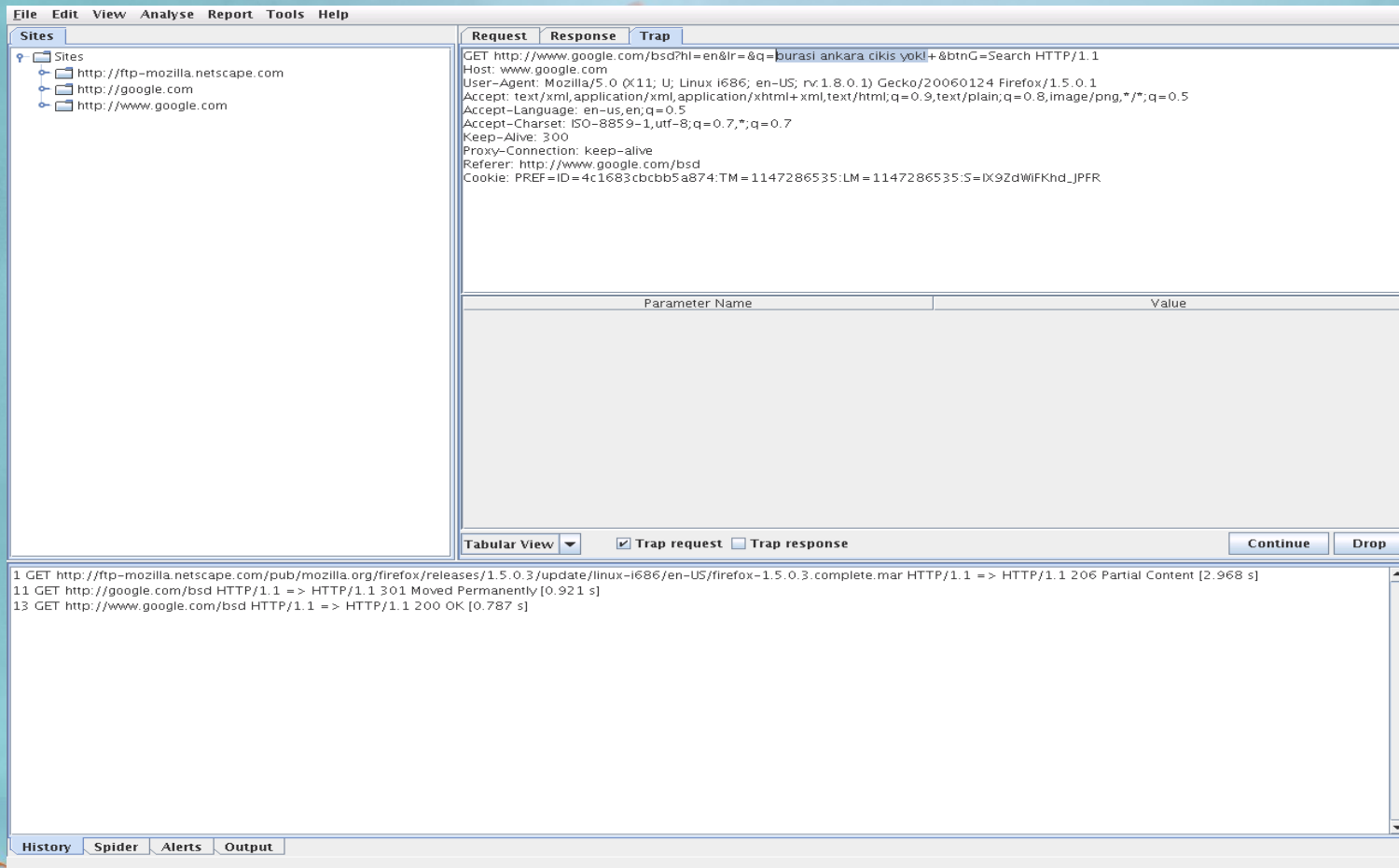
GET http://www.google.com/bsd?hl=en&lr=&q=Linux+Senlikleri+&btnG=Search HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.1) Gecko/20060124 Firefox/1.5.0.1
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://www.google.com/bsd
Cookie: PREF=ID=4c1683cbcbb5a874:TM=1147286535:LM=1147286535:S=IX92dWfKhd_JPFR

Below the request details is a table with two columns: 'Parameter Name' and 'Value'. The table is currently empty. At the bottom of the main window, there are checkboxes for 'Trap request' (checked) and 'Trap response' (unchecked), along with 'Continue' and 'Drop' buttons. The bottom status bar shows a 'History' tab with a list of three requests:

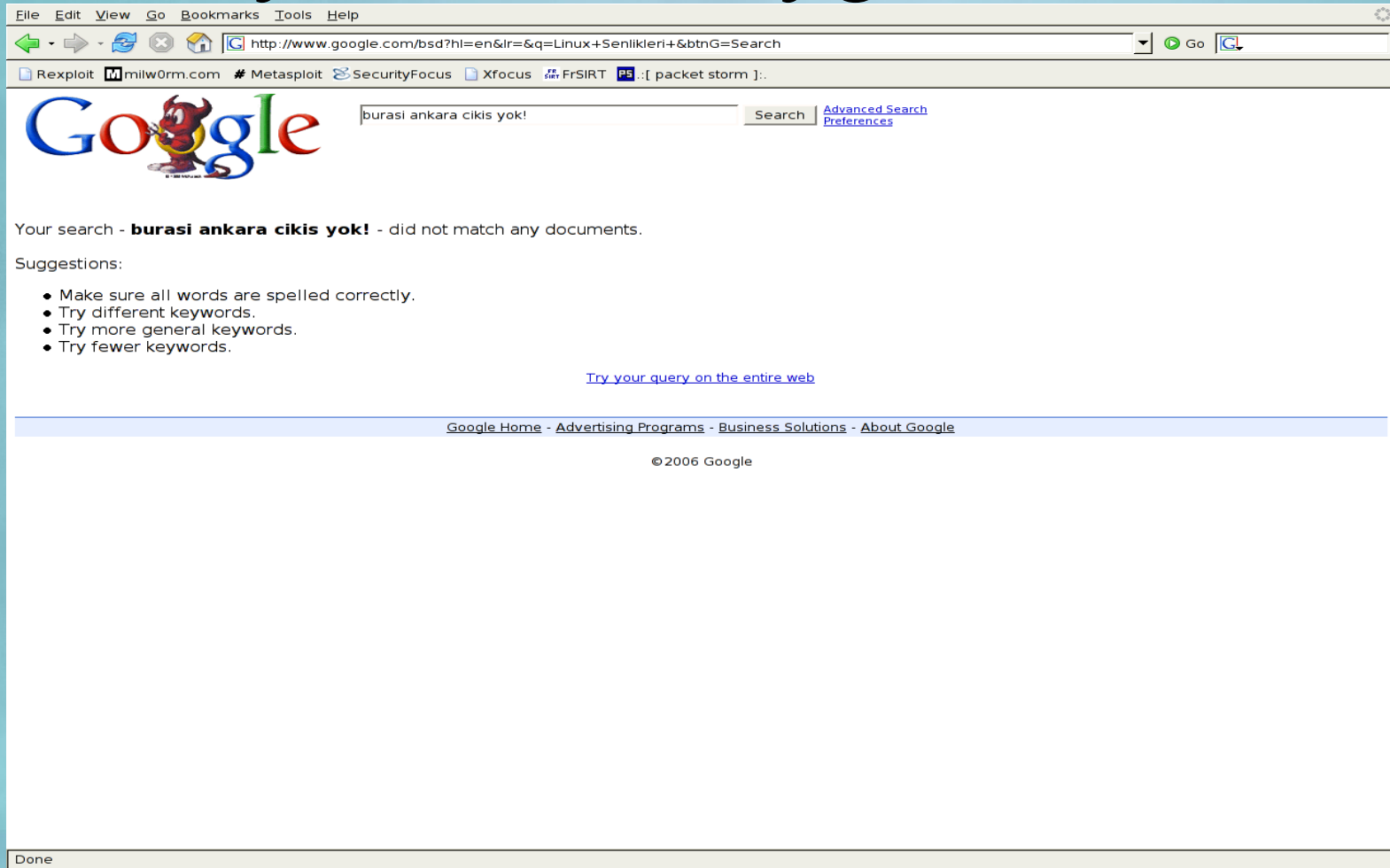
- 1 GET http://ftp-mozilla.netscape.com/pub/mozilla.org/firefox/releases/1.5.0.3/update/linux-i686/en-US/firefox-1.5.0.3.complete.mar HTTP/1.1 => HTTP/1.1 206 Partial Content [2.968 s]
- 11 GET http://google.com/bsd HTTP/1.1 => HTTP/1.1 301 Moved Permanently [0.921 s]
- 13 GET http://www.google.com/bsd HTTP/1.1 => HTTP/1.1 200 OK [0.787 s]

The bottom of the application has a 'Spider', 'Alerts', and 'Output' section.

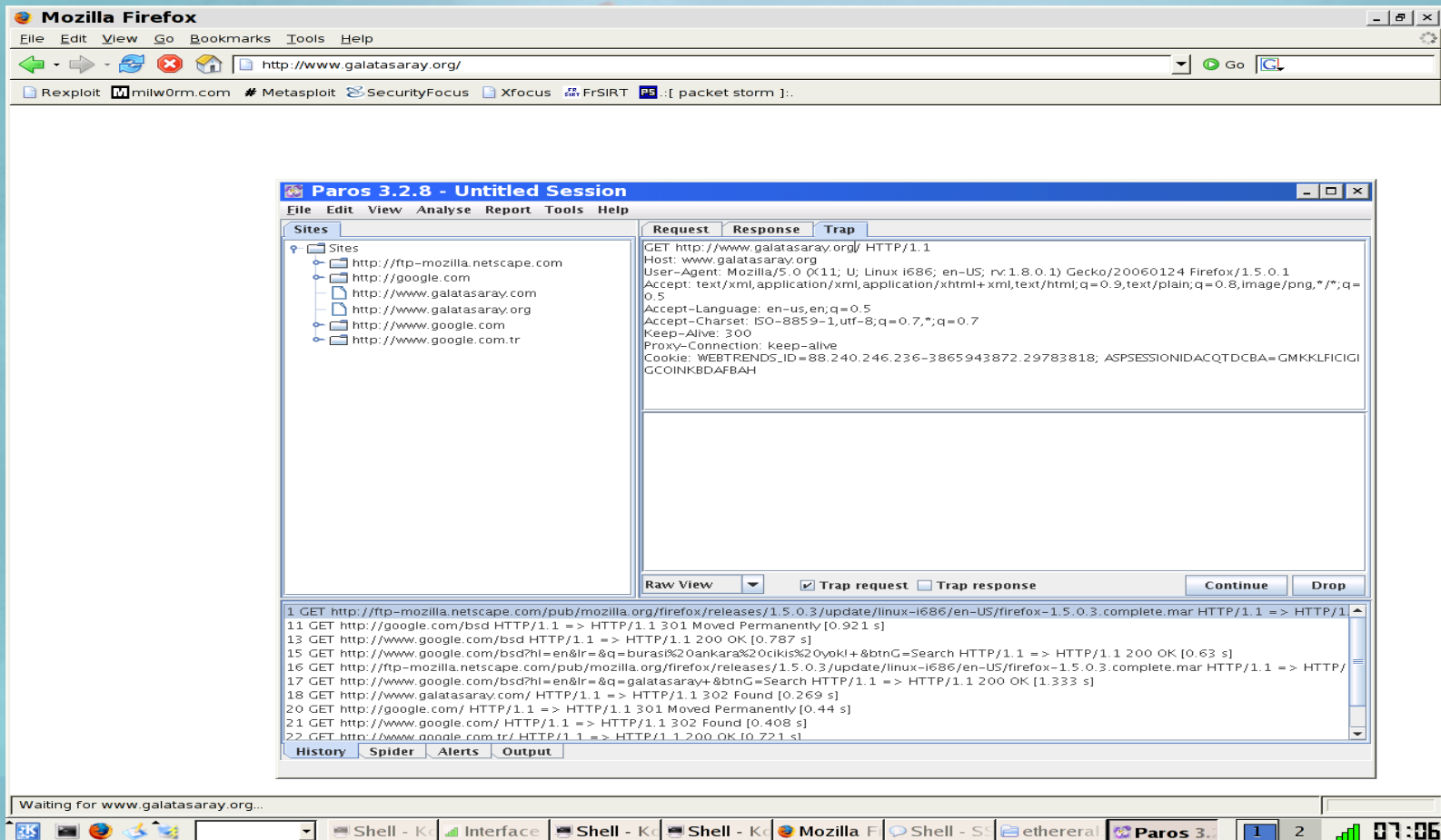
Araya Girme Uygulaması-3



Araya Girme Uygulamasi-4



Araya Girme Uygulamasi-5



Araya Girme Uygulamasi-6

Antu.com - İlk ve Tek Fenerbahçe Portalı - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.antu.com/default.aspx

Rexploit milw0rm.com # Metasploit SecurityFocus Xfocus FrSIRT [packet storm]:

Firefox prevented this site from opening a popup window. Preferences

Şampiyonluğa Kalan Süre

FENERBAHÇE TARAF TARAFININ RESMİ SİTESİ Fenerbahçe Foto Galerisi Multimedia FenerTV Forum Online Chat Fenerlist Email Antu Baby

Tüm Haberler

Kafitemiz Denizli'de
Takımımız "Şampiyonluk" için yola çıktı
Hazırlıklar Tamamlandı...!
Fenerbahçe 72-74 Efes Pilsen
Selçuk'un Sözleşmesi 2 Yıl Uzatıldı
Alex'in Golü "Top 10" da
Abdi İpekçi Deimalı...
Denizli Valisi'nin Açıklaması
Sadettin Saran'dan Zamansız Bir Çıkış
Alt Yapı Demeli'nin Denizli Deplasman O...
Başkanımız: "Gündemimizde transfer değil.
Şampiyonluk Maçımızın Hakemi Belli Oldu
"İlk Kongrede Başkanlığa Adayım"
Antu.com'dan Giriş Introsunun Mp3'ü

Paros 3.2.8 - Untitled Session

File Edit View Analyse Report Tools Help

Sites

- http://ftp-mozilla.netscape.com
- http://google.com
- http://www.antu.com
- http://www.galatasaray.com
- http://www.galatasaray.org
- http://www.google.com
- http://www.google.com.tr

Request Response Trap

Raw View ☐ Trap request ☐ Trap response Continue

1 GET http://ftp-mozilla.netscape.com/pub/mozilla.org/firefox/releases/1.5.0.3/update/linux-i686/en-US/firefox-1.5.0.3.complete.mar HTTP/1.1 => HTTP/1.1 301 Moved Permanently [0.921 s]
11 GET http://google.com/bsd HTTP/1.1 => HTTP/1.1 200 OK [0.787 s]
13 GET http://www.google.com/bsd?hl=en&lr=&q=buras%20ankara%20cikis%20yokl+&btnG=Search HTTP/1.1 => HTTP/1.1 200 OK [0.63 s]
15 GET http://ftp-mozilla.netscape.com/pub/mozilla.org/firefox/releases/1.5.0.3/update/linux-i686/en-US/firefox-1.5.0.3.complete.mar HTTP/1.1 => HTTP/1.1 301 Moved Permanently [0.44 s]
16 GET http://www.google.com/bsd?hl=en&lr=&q=galatasaray+&btnG=Search HTTP/1.1 => HTTP/1.1 200 OK [1.333 s]
17 GET http://www.galatasaray.com/ HTTP/1.1 => HTTP/1.1 302 Found [0.269 s]
18 GET http://www.google.com/ HTTP/1.1 => HTTP/1.1 301 Moved Permanently [0.44 s]
20 GET http://www.google.com/ HTTP/1.1 => HTTP/1.1 302 Found [0.408 s]
21 GET http://www.google.com/tr/ HTTP/1.1 => HTTP/1.1 200 OK [0.721 s]
22 GET http://www.google.com/tr/ HTTP/1.1 => HTTP/1.1 200 OK [0.721 s]

Transferring data from www.antu.com...

Shell - K Shell - K Shell - K Antu.com Shell - S etheral Paros 3.2 01:07

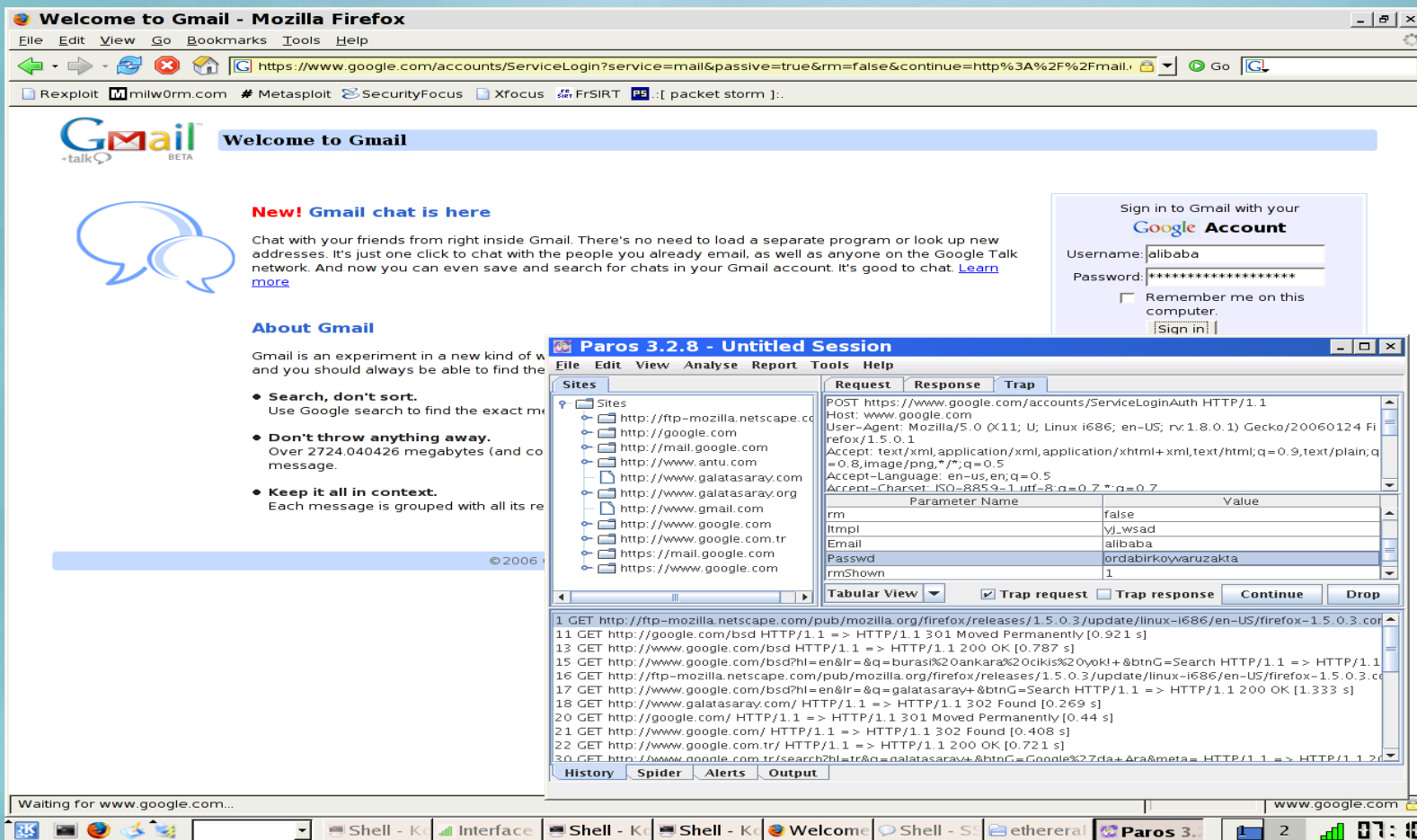
2. Katmanda Guvenlik

- İletişimin başlangıç noktası, dolayısıyla en önemli katman.
- Arpwatch - Arp Gözlem Aracı
- SwarpMon – Switch Gözlem aracı
- Yönetilebilir switch kullanmak ve MAC security, VLAN özelliklerini aktif hale getirmek

Şifreli Trafik Ne kadar Güvenli?

- Dinlemeye karşı en etkin çözüm:Şifreleme
- Peki şifreleme Ne kadar güvenli ?
- Sertifika otorite kavramı(CA)
- Şifreleme kullanırken dikkat+bilgi
 - Her sorulan soruya Yes! denmez!
- Ettercap, Cain & Abel vs
- Banka Örneği...

Şifreli trafikte Araya Girme



HTTPS Trafigi Degistirme

Sign In - Mozilla Firefox

Dosya Düzen Görünüm Glt Yvr İmleri Araçlar Yardım

http://login.live.com/login.srf?id=28svc=mail&cbid=243258msppjph=1&tw=0&fs=1&fsa=1&fsat=1296000&lang=EN&lc=1033

İlk Adım Haberler

Home | My MSN | Shopping | Money | People & Chat

Search

msn Hotmail

What's new For Free Hotmail? MSN Hotmail Inbox Storage is now 250 MB and there is an increased attachment size of 10 MB!

New to MSN Hotmail?

A smarter way to email – FREE!

- **Get enhanced security for your email!**
Help keep your inbox free from contamination. With powerful spam filters and enhanced virus scanning & cleaning.
- **Easily connect & share!**
Send & receive e-mail from any Web connection. With a huge 250MB inbox* and the ability to send up to 10MB files or photos.
- **Express yourself!**
Have fun personalizing e-mail to friends & family. With unique emoticons, signatures, background choices, fonts & layout styles.

[Sign Up](#)

*250MB inbox available only in the 50 United States, District of Columbia, and Puerto Rico. Eligible Hotmail users will first receive 25MB at sign-up. Please allow at least 30 days for activation of your 250MB storage to verify your e-mail account and help prevent abuse. Microsoft Corporation reserves the right to provide 250MB inbox to free Hotmail accounts at its discretion.

Sign In to Hotmail

Help

E-mail address:

Password:
[Forgot your password?](#)

[Sign In](#)

☐ Save my e-mail address and password

☒ Save my e-mail address

☐ Always ask for my e-mail address and password

[Sign in using enhanced security](#)

Windows Live ID

Works with Windows Live, MSN, and Microsoft Passport sites

[Account Services](#) | [Privacy Statement](#) | [Terms of Use](#)

© 2006 Microsoft Corporation. All rights reserved.

©2006 Microsoft Corporation MSN Privacy & Legal About

Tamam

HTTPS Trafigi Degistirme

Doğya Düzen Görünüm Git Yer İmleri Araçlar Yardım

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

İlk Adım Haberler

Home | My MSN | Shopping | Money | People & Chat

Search

msn Hotmail

What's new For Free Hotmail? MSN Hotmail Inbox Storage is now 250 MB and there is an increased attachment size of 10 MB!

New to MSN Hotmail?
A smarter way to email – FREE!

- Get enhanced security for your email!**
Help keep your inbox free from contamination. With powerful spam filters and enhanced virus scanning & cleaning.
- Easily connect & share!**
Send & receive e-mail from any Web connection. With a huge 250MB inbox* and the ability to send up to 10MB files or photos.
- Express yourself!**
Have fun personalizing e-mail to friends & family. With unique emoticons, signatures, background choices, fonts & layout styles.

[Sign Up](#)

*250MB inbox available only in the 50 United States, District of Columbia, and Puerto Rico. Eligible Hotmail users will first receive days for activation of your 250MB storage prevent abuse. Microsoft Corporation reserves the right to change these terms at its discretion.

Sign In to Hotmail Help

E-mail address: rastgele@hotmail.com

Password: *****
[Forgot your password?](#)

[Sign In](#)

☐ Save my e-mail address and password
☒ Save my e-mail address
☐ Always ask for my e-mail address and password
[Sign in using enhanced security](#)

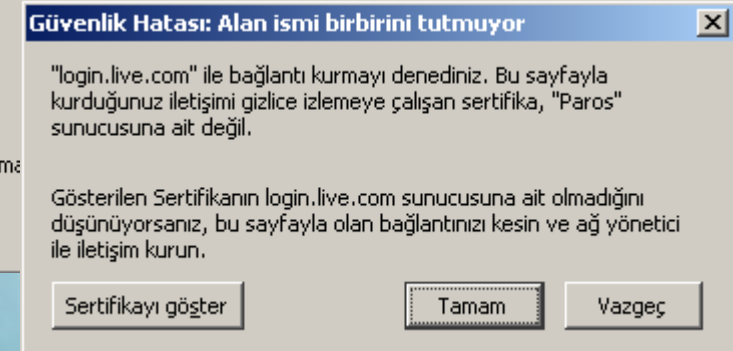
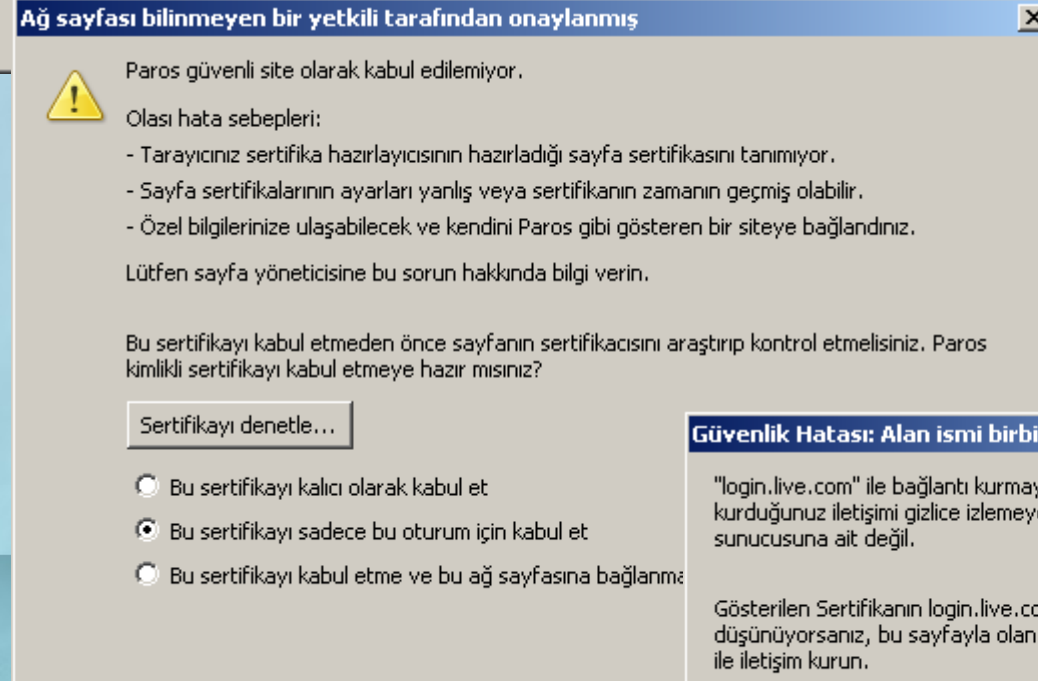
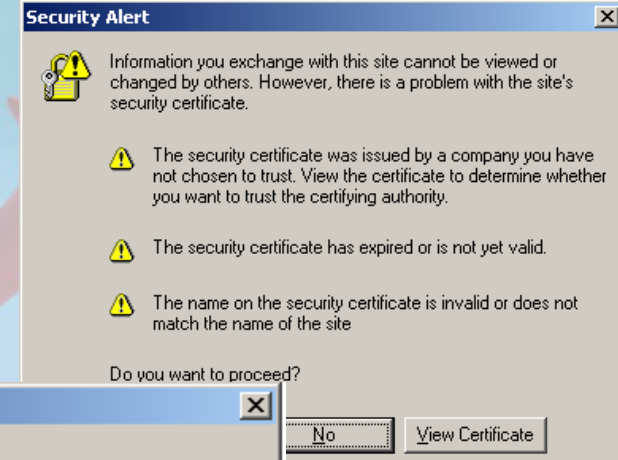
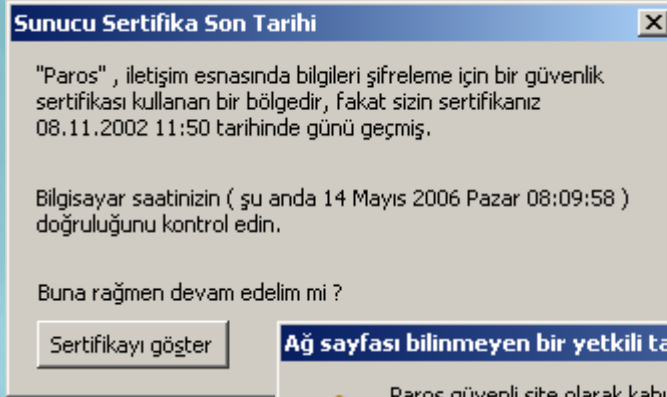
Paros - Untitled Session

File Edit View Analyse Report Tools Help

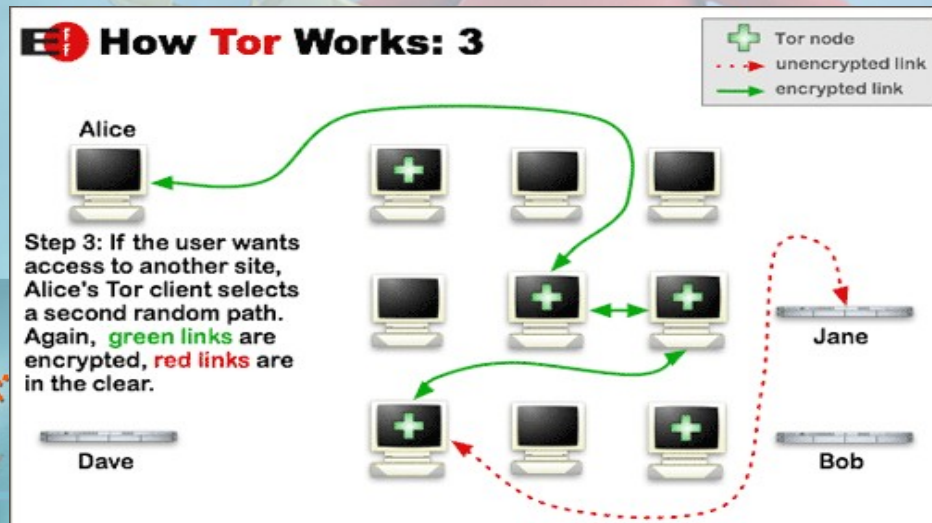
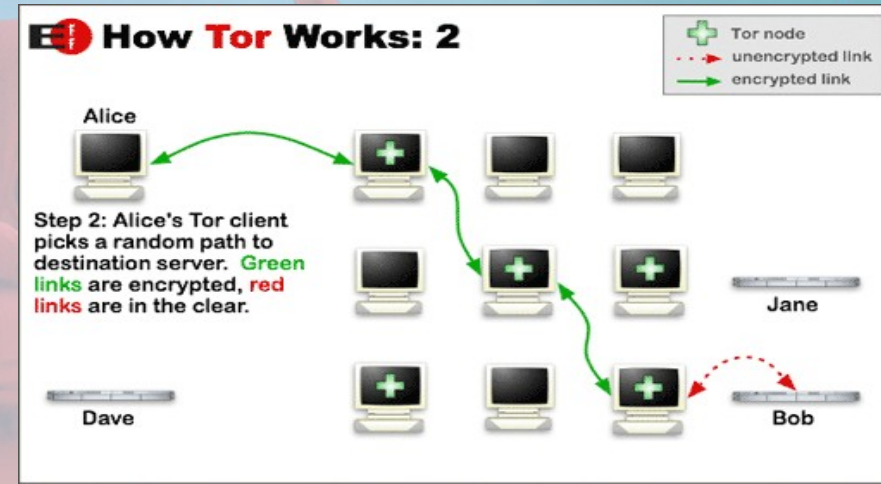
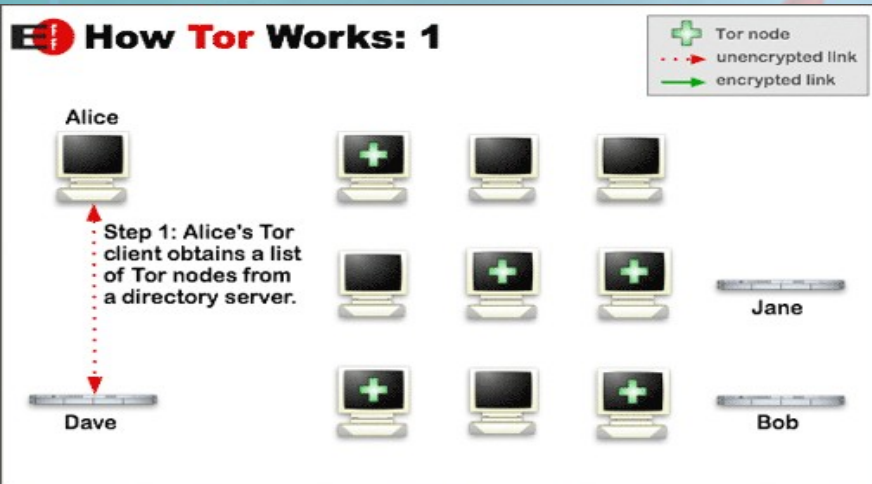
Sites	Request	Response	Trap														
Sites	POST https://login.live.com/ppsecure/post.srf?id=2&svc=mail&cbid=24325&msppjph=1&tw=0&fs=1&fsa=1&fsat=1296000&_lang=EN&lc=1033&bk=1147582792 HTTP/1.1 Host: login.live.com User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; tr; rv:1.8.0.3) Gecko/20060426 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																
	<table border="1"><thead><tr><th>Parameter Name</th><th>Value</th></tr></thead><tbody><tr><td>PPSX</td><td>Pa</td></tr><tr><td>PwdPad</td><td>IFYouAreReadingThisYouHaveTooM</td></tr><tr><td>login</td><td>rastgele@hotmail.com</td></tr><tr><td>passwd</td><td>bugun_pazar</td></tr><tr><td>LoginOptions</td><td>2</td></tr><tr><td>PPFT</td><td>Btr3IdQCIswovObWtUAdpyM5*f0xK0IecIn92KMPi0Bd55Yh3s7bO72Iq9BdEweQa5EIJ...</td></tr></tbody></table>			Parameter Name	Value	PPSX	Pa	PwdPad	IFYouAreReadingThisYouHaveTooM	login	rastgele@hotmail.com	passwd	bugun_pazar	LoginOptions	2	PPFT	Btr3IdQCIswovObWtUAdpyM5*f0xK0IecIn92KMPi0Bd55Yh3s7bO72Iq9BdEweQa5EIJ...
Parameter Name	Value																
PPSX	Pa																
PwdPad	IFYouAreReadingThisYouHaveTooM																
login	rastgele@hotmail.com																
passwd	bugun_pazar																
LoginOptions	2																
PPFT	Btr3IdQCIswovObWtUAdpyM5*f0xK0IecIn92KMPi0Bd55Yh3s7bO72Iq9BdEweQa5EIJ...																
Tabular Vi... <input checked="" type="checkbox"/> Trap request <input type="checkbox"/> Trap response Continue Drop																	

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 https://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 HTTP/1.1 => HTTP/1.1 302 Found [0.631 s]

Firefox/Internet Explorer?



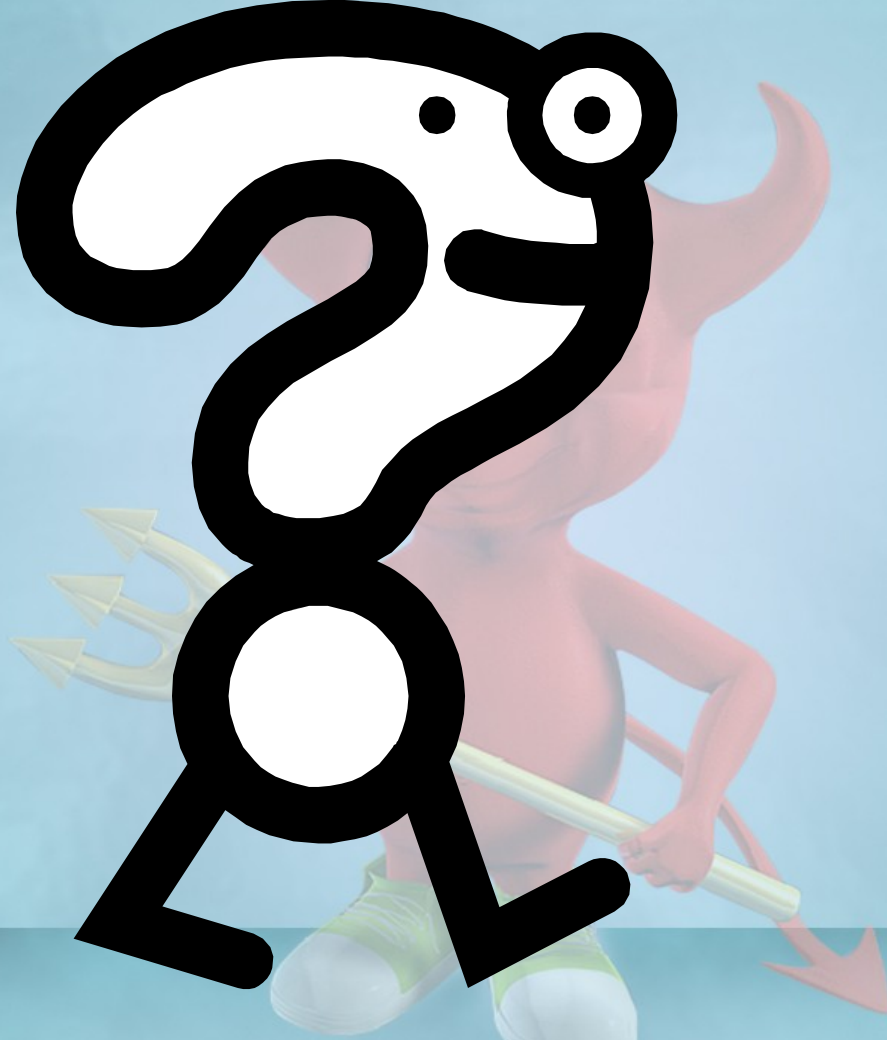
Tor ile güvenli sörf!



!Sonuc

- Eğitim Şart ;-)
- Türkiye Güvenlik eğitimleri
- Kitap, Belge, Yayınlar..
 - Açık Akademi Yayınları – Güvenlik Kitapları
 - Ağ güvenliği ipucları
 - TCP/IP Güvenliği
 - Pengvence Dergisi
 - Olympos Security(www.olympos.org)
 - EnderUNIX.org

Sorularınız



Teşekkürler..