BİLGİ GÜVENLİĞİ AKADEMİSİ

www.bga.com.tr

Derinlemesine Paket İnceleme/Deep Packet Inspection

@2014

Örnek Eğitim Notu

bilgi@bga.com.tr

Bölüm İçeriği

- Saldırı ve anormallik tespit sistemleri
  - Çalışma yapıları
  - Paket karekteristiği algılama
  - Diğer güvenlik sistemlerinden temel farklılıkları
- Açık kod IPS/ADS sistemleri
  - BroIDS
  - Snort IDS
- Saldırı tespit sistemi imzaları nasıl geliştirilir?
- Saldırı tespit sistemleri kötücül yazılımlar tarafından nasıl atlatılır?
- Saldırı tespit sistemleri ve şifreli trafik
- Yakalanan paketlerden orjinal verilerin elde edilmesi
- Ağ trafiğinde kelime bazlı izleme
- Uygulama seviyesi protokollerin pasif olarak izlenmesi

DPI(Deep Packet Inspection) Örneği

Hatalı IPS Kuralı

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (\
msg:"ET P2P ABC Torrent User-Agent (ABC/ABC-3.1.0)"; \
flow:to_server,established; \
content:"User-Agent\: ABC/ABC"; nocase; \
sid:2003475;)
```


Doğru IPS Kuralı (DPI Destekli)

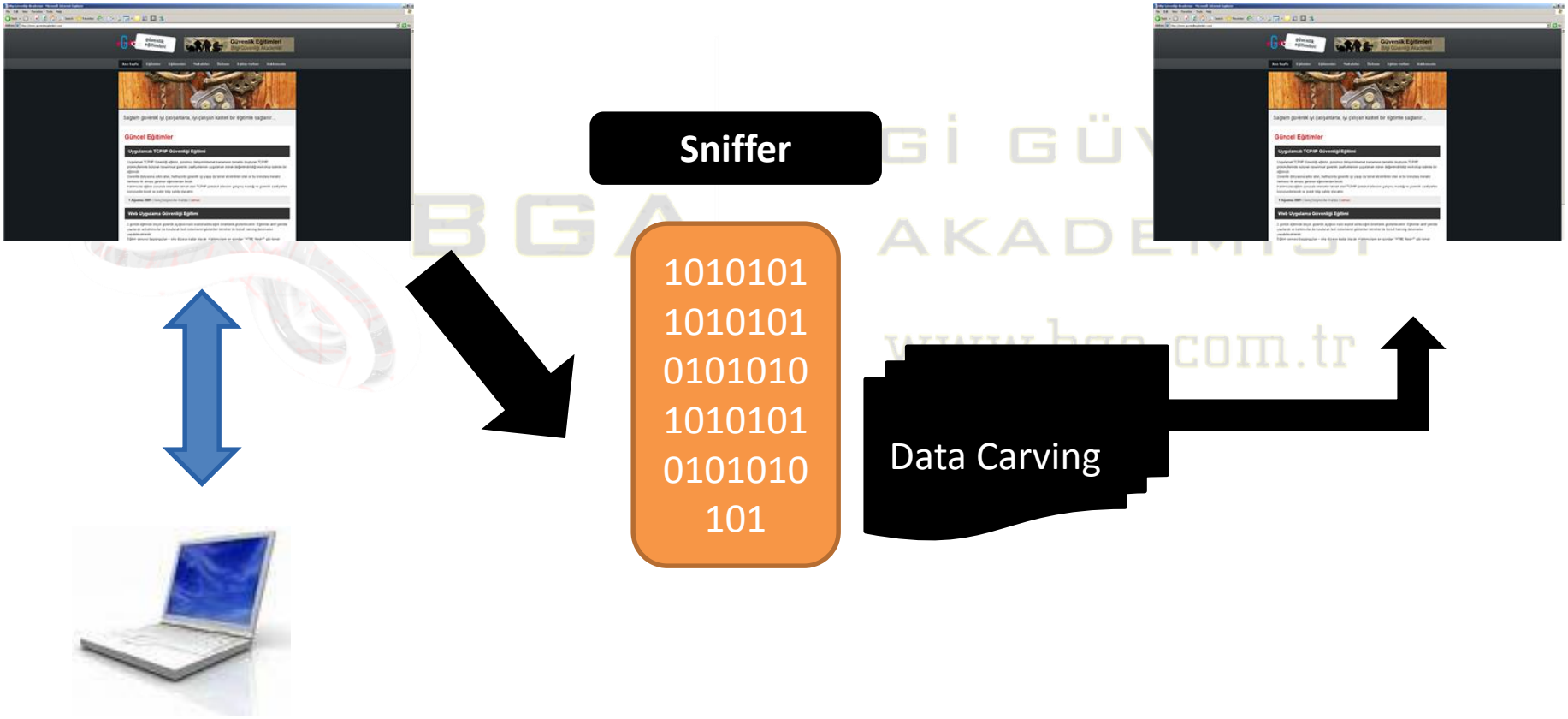
```
alert http $HOME_NET any -> $EXTERNAL_NET any (\
msg:"ET P2P ABC Torrent User-Agent (ABC/ABC-3.1.0)"; \
header.useragent:"ABC/ABC"; \
sid:2003475;)
```

Network Data Carving

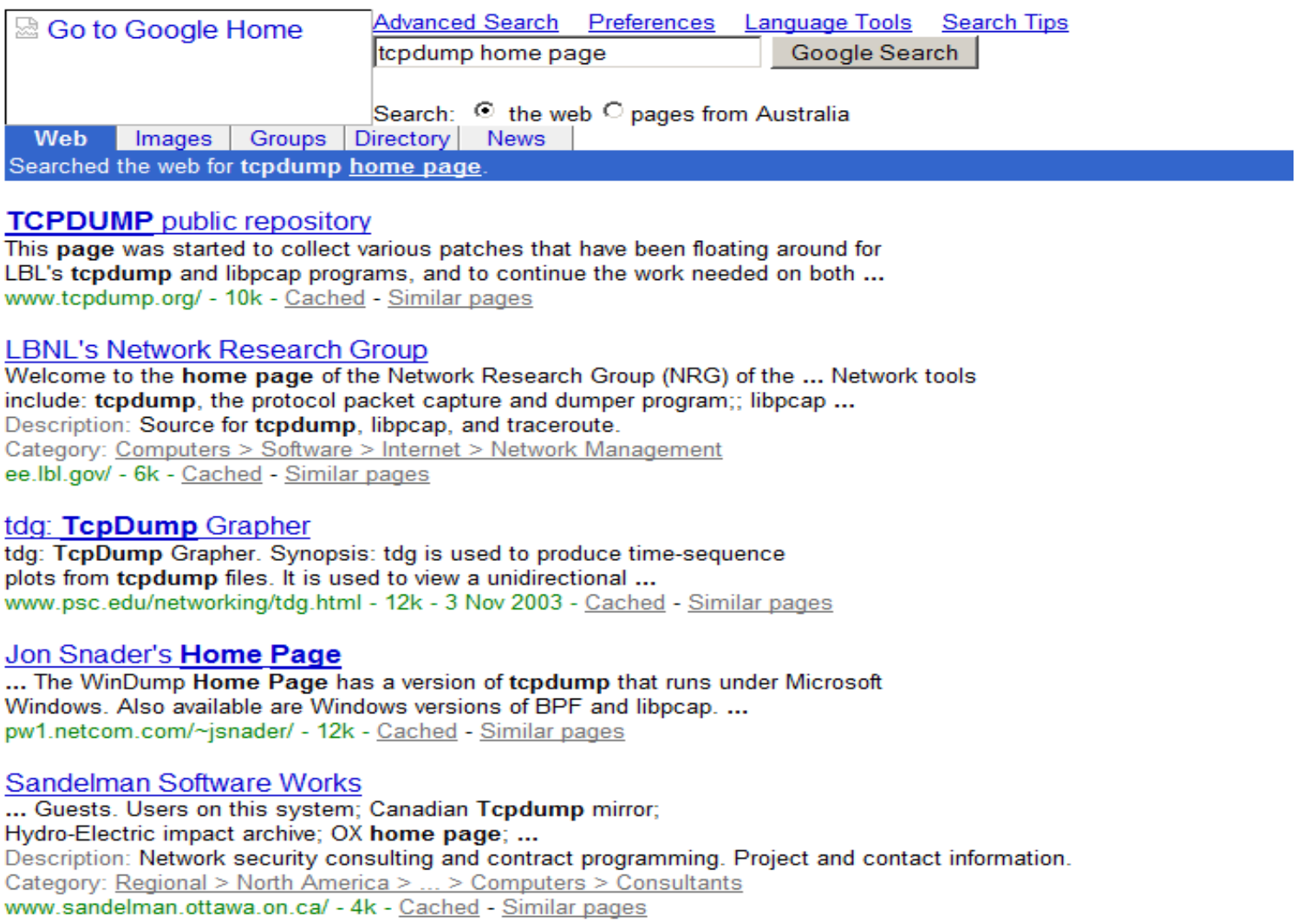
- Sniffer kullanarak kaydedilmiş binary dosyalardan(.pcap formatında veya farklı formatlarda) orjinal veri elde etmek
- Akan ağ trafiği üzerinde belirli şartlara göre izleme yapma
  - Echelon mantığı
  - Günümüzdeki DLP sistemlerinin atası sayılabilir.
- İki uç haberleşirken aradaki dinleme sistemleri iki uç ne görüyorsa aynısını görebilir, dinleyebilir ve kaydedebilir.
- Network forensic çalışmalarının temelini oluşturur.

Data Carving…

- Ham veriden orijinal veri elde etme yöntemi



ChaosReader



Chaosreader:Telnet-replay

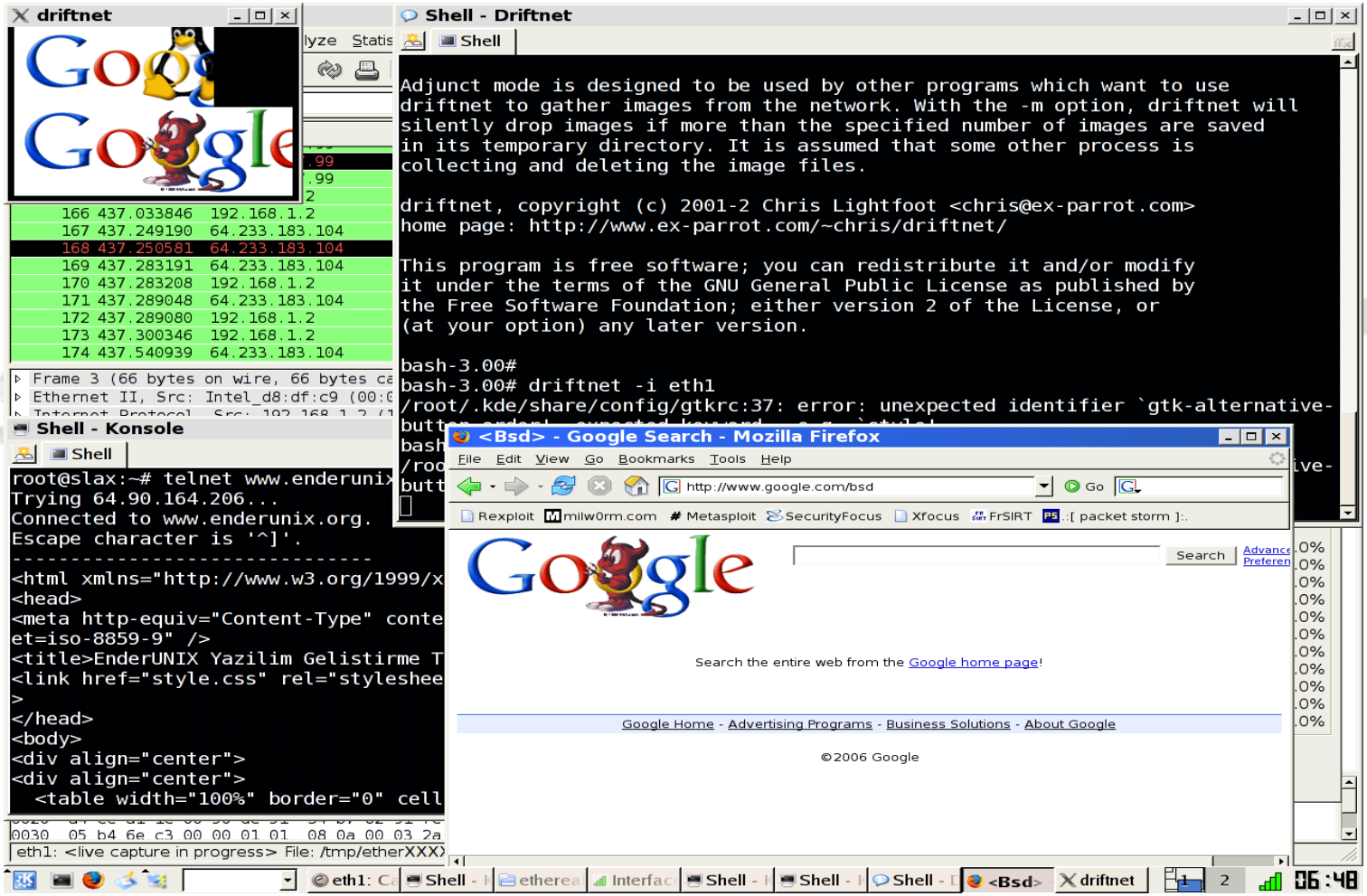
```
Ubuntu 8.10
guvenlikod login: huzeyfe
Password:
Linux trcell 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
$ ls
chaosreader0.94  telnet.pcap
$ id
uid=1001(huzeyfe) gid=1001(huzeyfe) groups=1001(huzeyfe)
```

```
root@guvenlikod:/home/huzeyfe# tcpdump -s 0 tcp port 23 -w telnet.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C87 packets captured
87 packets received by filter
0 packets dropped by kernel
```

Telnet Replay-II

```
root@guvenlikod:/home/huzeyfe# perl chaosreader0.94 telnet.pcap
$* is no longer supported at chaosreader0.94 line 265.
Chaosreader ver 0.94

Opening, telnet.pcap

Reading file contents,                    100% (7123/7123)7/7123)99/7123)99/7123)10 100% (85/87)92% (80/87)
R 74% (64/87)packets, 55% (48/87)         37% (32/87)          18% (16/87)           0% (0/87)
Creating files...
   Num  Session (host:port <=> host:port)              Service
  0001  10.200.43.145:6501,10.200.169.163:23          telnet

index.html created.
root@guvenlikod:/home/huzeyfe# ls
chaosreader0.94  httplog.text  index.html  session_0001.telnet.html    telnet.pcap
getpost.html     image.html    index.text  session_0001.telnet.replay
root@guvenlikod:/home/huzeyfe# ./session_0001.telnet.replay 2
ÿýýý ÿý#ÿý'ÿýýûýýýûýú ÿðýú'ÿðýúýðýýýûýý!Ubuntu 8.10
guvenlikod login: PuTTYguvenlikod login: huzeyfe
Password:
Linux trcell 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
$ ls
chaosreader0.94  telnet.pcap
$ id
uid=1001(huzeyfe) gid=1001(huzeyfe) groups=1001(huzeyfe)
root@guvenlikod:/home/huzeyfe# PuTTY
```

Driftnet

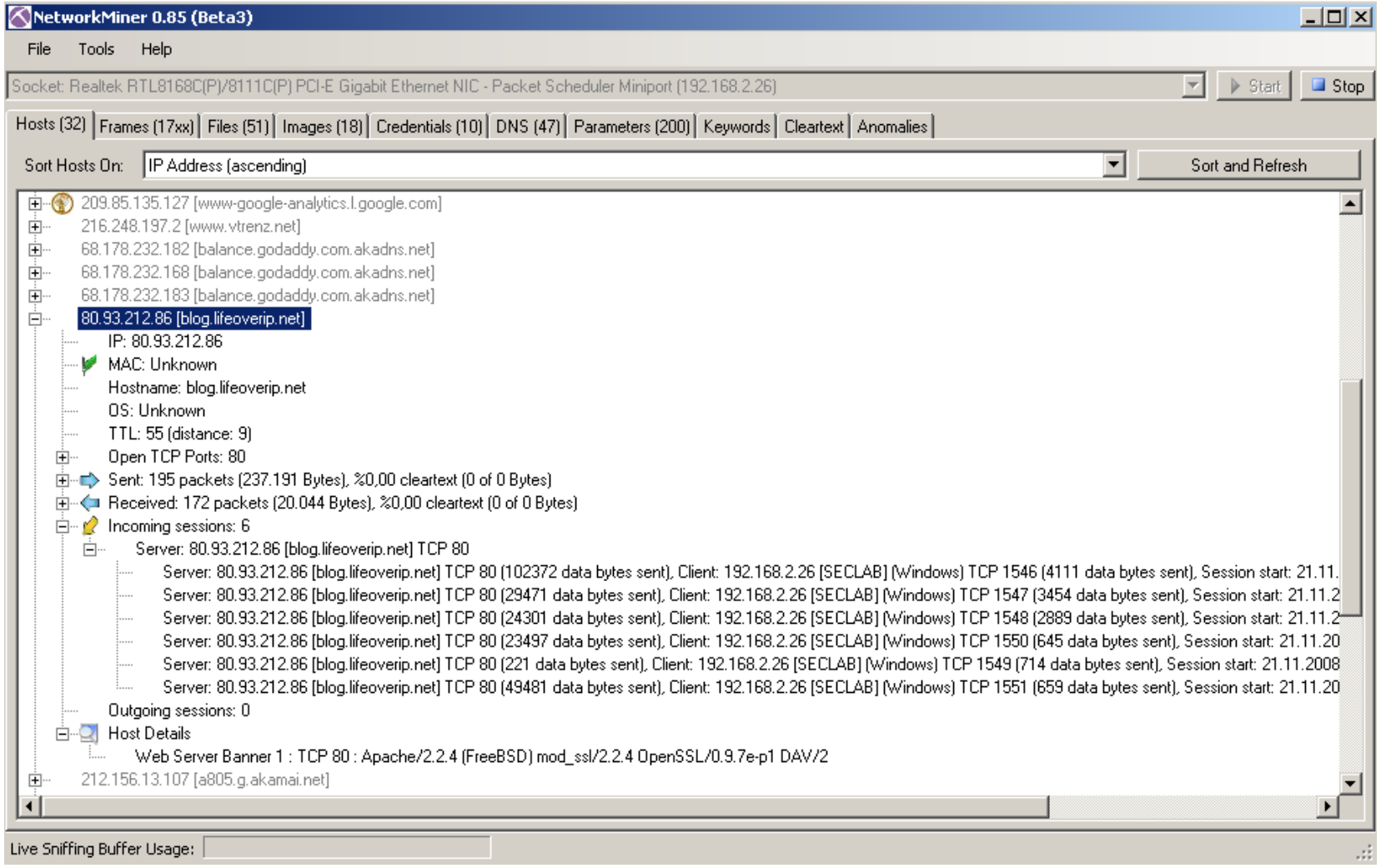

driftnet
Shell - Driftnet
Shell
Adjunct mode is designed to be used by other programs which want to use
driftnet to gather images from the network. With the -m option, driftnet will
silently drop images if more than the specified number of images are saved
in its temporary directory. It is assumed that 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.
bash-3.00#
bash-3.00# driftnet -i eth1
/root/.kde/share/config/gtkrc:37: error: unexpected identifier `gtk-alternative-
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
Frame 3 (66 bytes on wire, 66 bytes ca
Ethernet II, Src: Intel_d8:df:c9 (00:0
Shell - Konsole
Shell
root@slax:~# telnet www.enderunix
Trying 64.90.164.206...
Connected to www.enderunix.org.
Escape character is '^]'.
<html xmlns="http://www.w3.org/1999/x
<head>
<meta http-equiv="Content-Type" conte
et=iso-8859-9" />
<title>EnderUNIX Yazilim Gelistirme T
<link href="style.css" rel="styleshee
>
</head>
<body>

<table width="100%" border="0" cell
0030 05 b4 6e c3 00 00 01 01 08 0a 00 03 2a
eth1: <live capture in progress> File: /tmp/etherXXX
<Bsd> - Google Search - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.google.com/bsd
Go
Rexploit milw0rm.com Metasploit SecurityFocus Xfocus FrSIRT :[packet storm]:.
Search
Search the entire web from the Google home page!
Google Home - Advertising Programs - Business Solutions - About Google
©2006 Google
eth1: C
Shell -
Shell -
Shell -
<Bsd>
driftnet
06:48

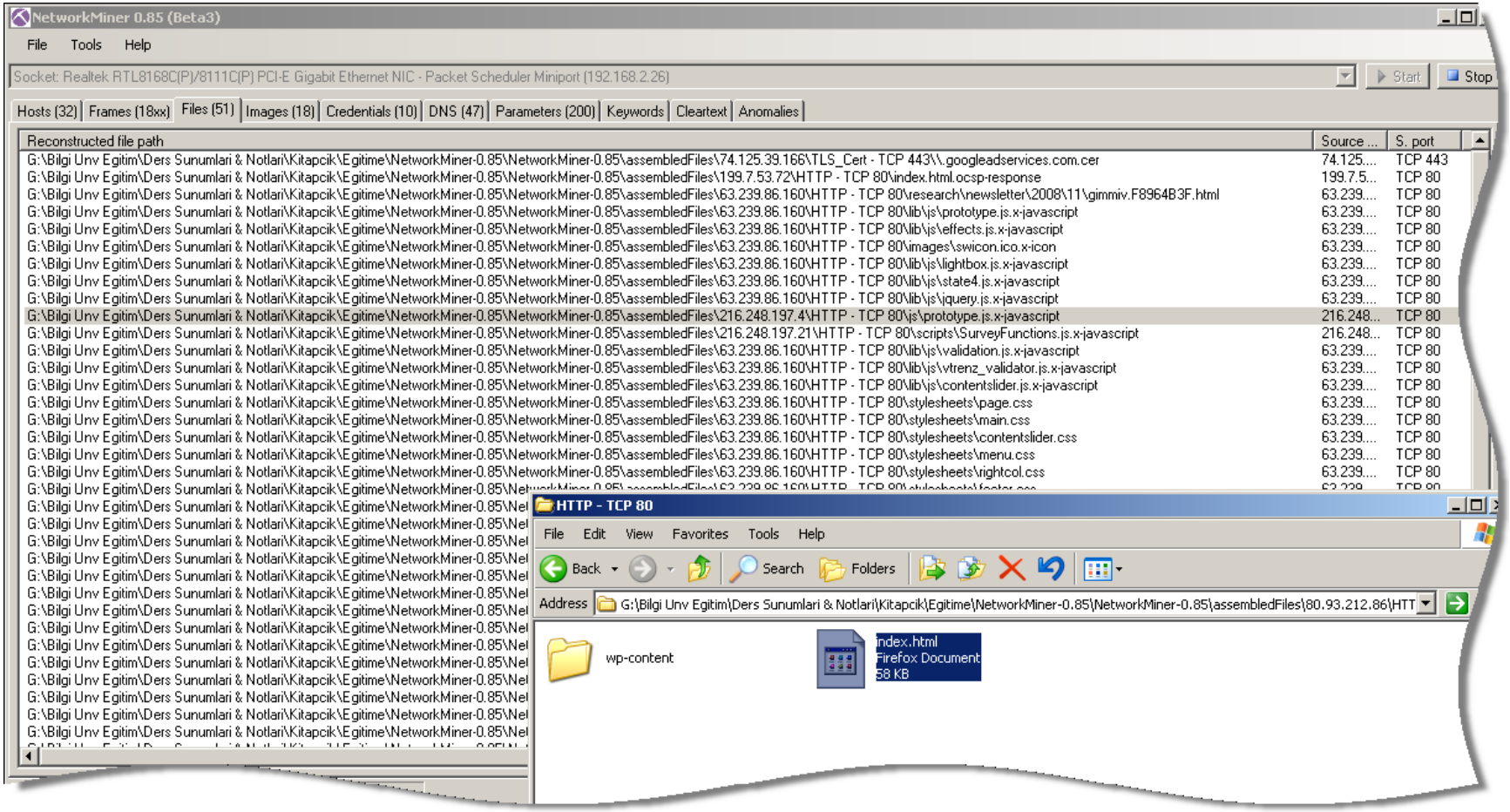
NetworkMiner

- Windows sistemler için geliştirilmiş ağ adli bilişim aracı
- Temel amacı ağ trafiğini yakalayarak (veya daha once kadedilmiş pcap dosyalarını kullanarak)trafik içerisinde geçen işe yarar bilgilerin ayıklanmasıdır.
- NetworkMiner kullanılarak HTTP, FTP ve SMB protokolleri üzerinden yapılan tüm dosya transferlerindeki objeler(resim, muzik, pdf vs) orjinalleri gibi ayıklanabilir.
- NetworkMiner uygulama seviyesi protokollerini ayıklayabilmek için port numaralarına bakarak işlem yapmaz(Port no 80 o zaman HTTP'dir gibi) aksine SPID (Statistical Protocol Identification) yöntemi kullanarak uygulama seviyesi protokollerini port bağımsız olarak tanımlayabilir.

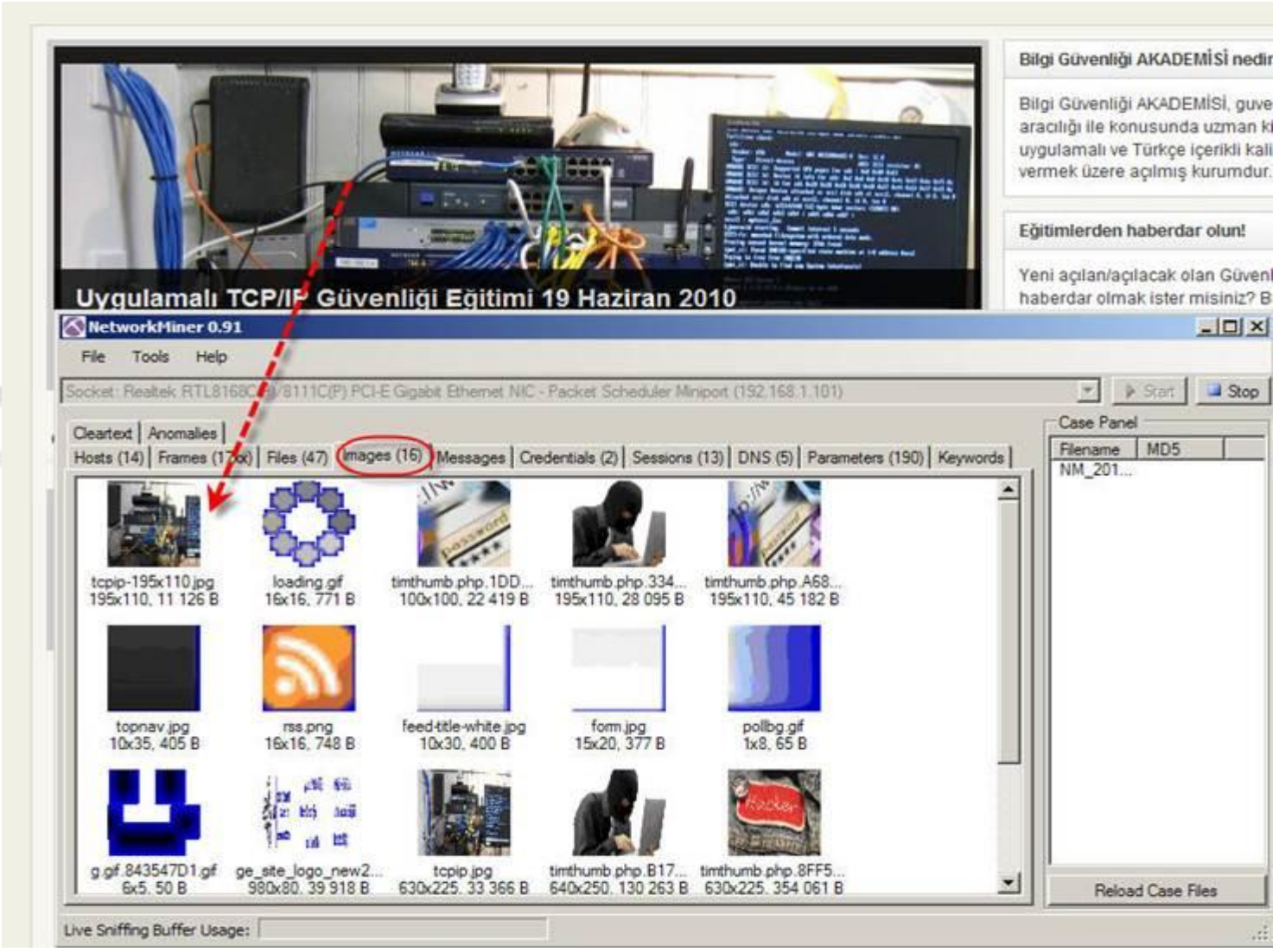
NetworkMiner-I



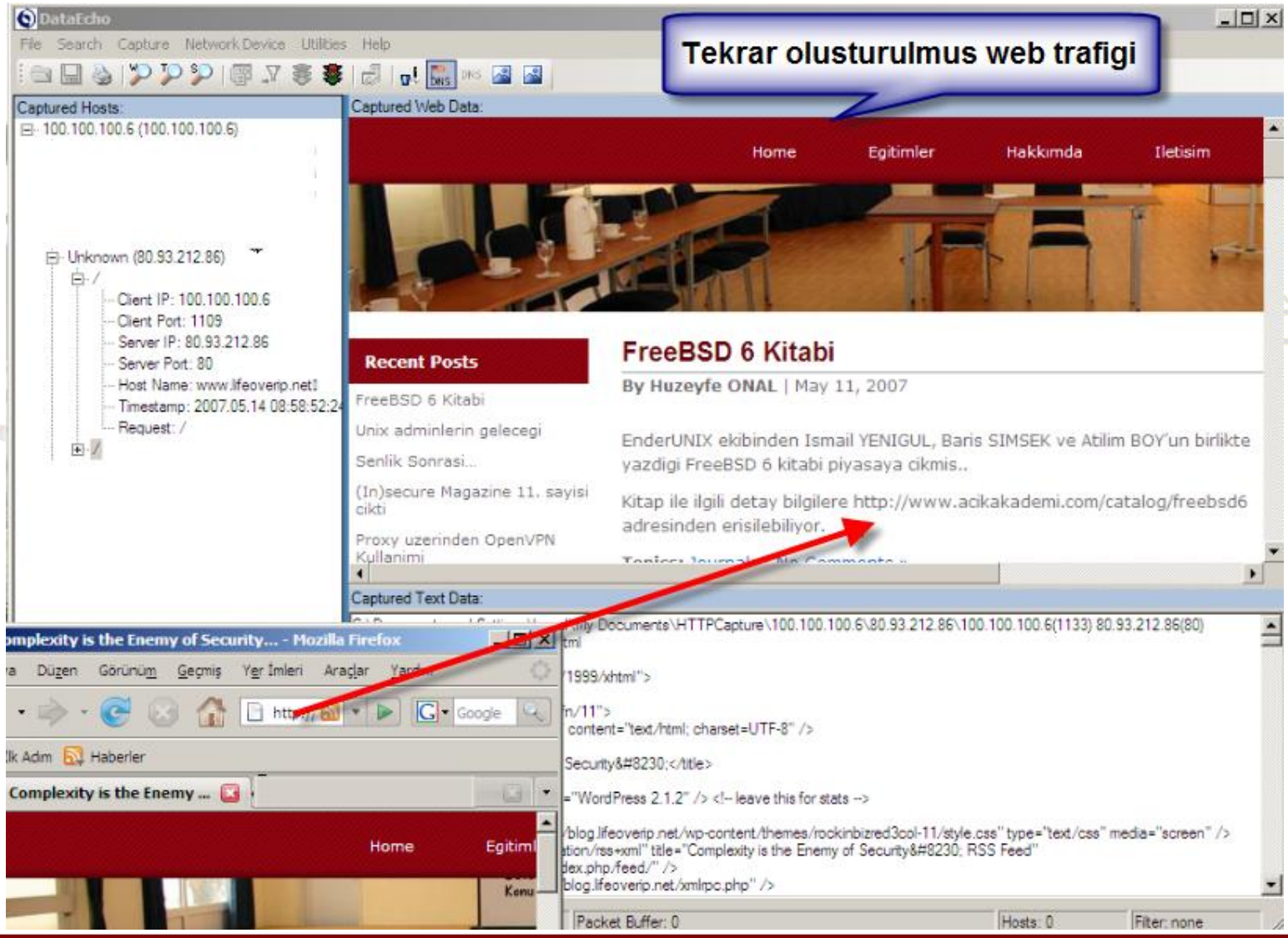
NetworkMiner-II



NetworkMiner-III



DataEcho Yazılımı



Tcpxtract

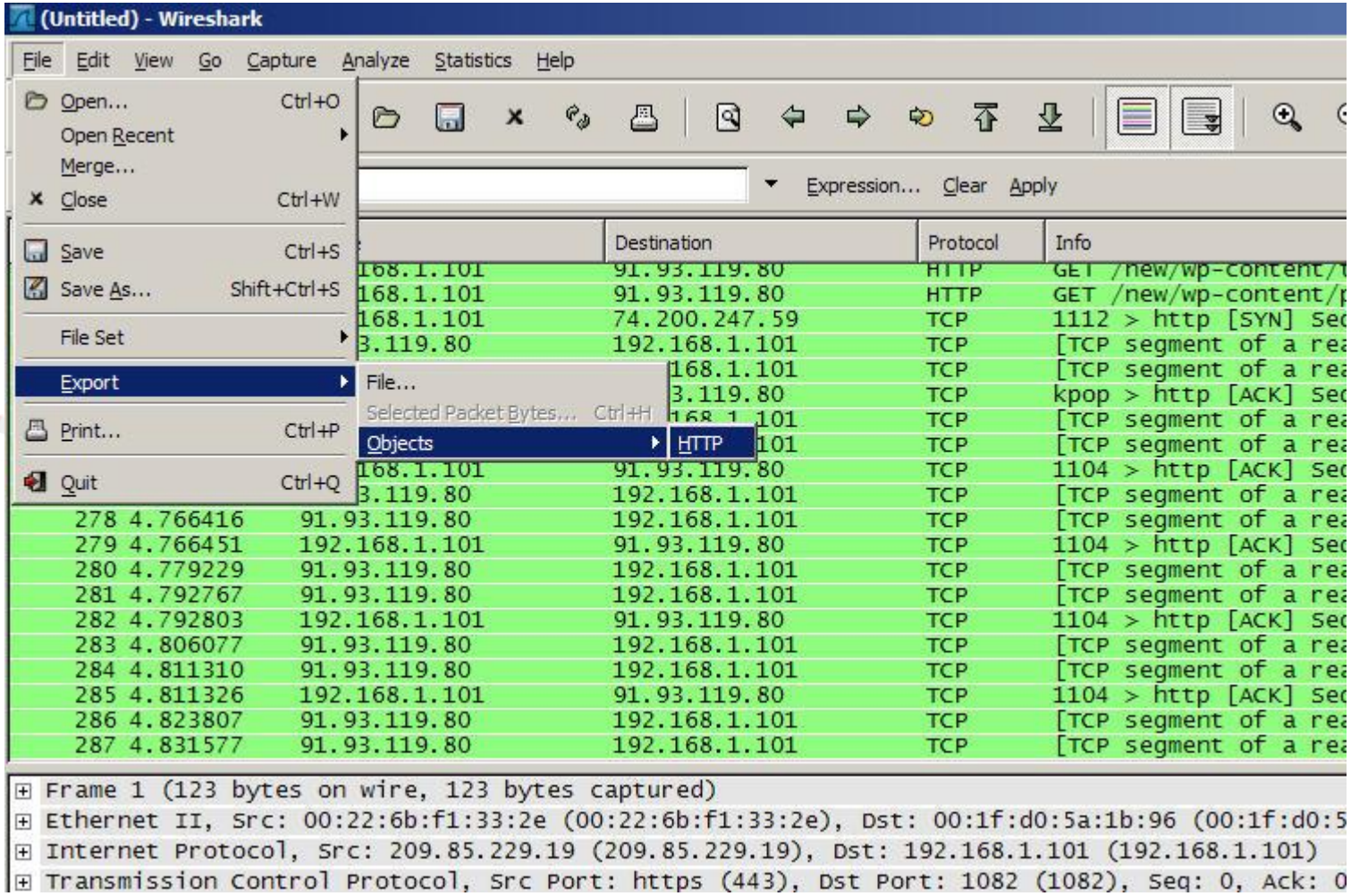
- Tüm dosya uzantıları için data carving uygulaması
- tcpxtract -f tcpdump-site.pcap -o pdf-dump

TcpXtract Dosya Tipi Tanımlama

- Ağ trafiğinden ayıklanmak istenen dosya tipi tcpxtract.conf dosyasında tanımlanmalıdır.

```
root@bt:~# head -25 /etc/tcpxtract.conf
#--------------------------------------------------------------------
# ANIMATION FILES
#--------------------------------------------------------------------
#

# AVI (Windows animation and DiVX/MPEG-4 movies)
avi(4000000, RIFF\?\?\?\?);

# MPEG Video
mpg(4000000, \x00\x00\x01\xba, \x00\x00\x01\xb9);
mpg(4000000, \x00\x00\x01\xb3, \x00\x00\x01\xb7);

# Macromedia Flash
fws(4000000, FWS);

#--------------------------------------------------------------------
# GRAPHICS FILES
#--------------------------------------------------------------------
#
#
# AOL ART files
art(150000,     \x4a\x47\x04\x0e, \xcf\xc7\xcb);
art(150000,     \x4a\x47\x03\x0e, \xd0\xcb\x00\x00);
```

Wireshark


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Open... Ctrl+O
Open Recent
Merge...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export
Print... Ctrl+P
Quit Ctrl+Q
File...
Selected Packet Bytes... Ctrl+H
Objects
HTTP
Expression... Clear Apply
Destination Protocol Info
278 4.766416 91.93.119.80 192.168.1.101 TCP [TCP segment of a rea
279 4.766451 192.168.1.101 91.93.119.80 TCP 1104 > http [ACK] Seq
280 4.779229 91.93.119.80 192.168.1.101 TCP [TCP segment of a rea
281 4.792767 91.93.119.80 192.168.1.101 TCP [TCP segment of a rea
282 4.792803 192.168.1.101 91.93.119.80 TCP 1104 > http [ACK] Seq
283 4.806077 91.93.119.80 192.168.1.101 TCP [TCP segment of a rea
284 4.811310 91.93.119.80 192.168.1.101 TCP [TCP segment of a rea
285 4.811326 192.168.1.101 91.93.119.80 TCP 1104 > http [ACK] Seq
286 4.823807 91.93.119.80 192.168.1.101 TCP [TCP segment of a rea
287 4.831577 91.93.119.80 192.168.1.101 TCP [TCP segment of a rea
Frame 1 (123 bytes on wire, 123 bytes captured)
Ethernet II, Src: 00:22:6b:f1:33:2e (00:22:6b:f1:33:2e), Dst: 00:1f:d0:5a:1b:96 (00:1f:d0:5
Internet Protocol, Src: 209.85.229.19 (209.85.229.19), Dst: 192.168.1.101 (192.168.1.101)
Transmission Control Protocol, Src Port: https (443), Dst Port: 1082 (1082), Seq: 0, Ack: 0

Xplico

- Network Forensic Analysis Tool (NFAT)
  - Network forensic analiz aracı
- Port Independent Protocol Identification (PIPI)
- Açık kaynak kodlu, ücretsiz kullanım hakkı
- Veri ayıklama özelliği
  - Webmail
  - IM
  - Facebook chat mesajları

Protocols Dissectors

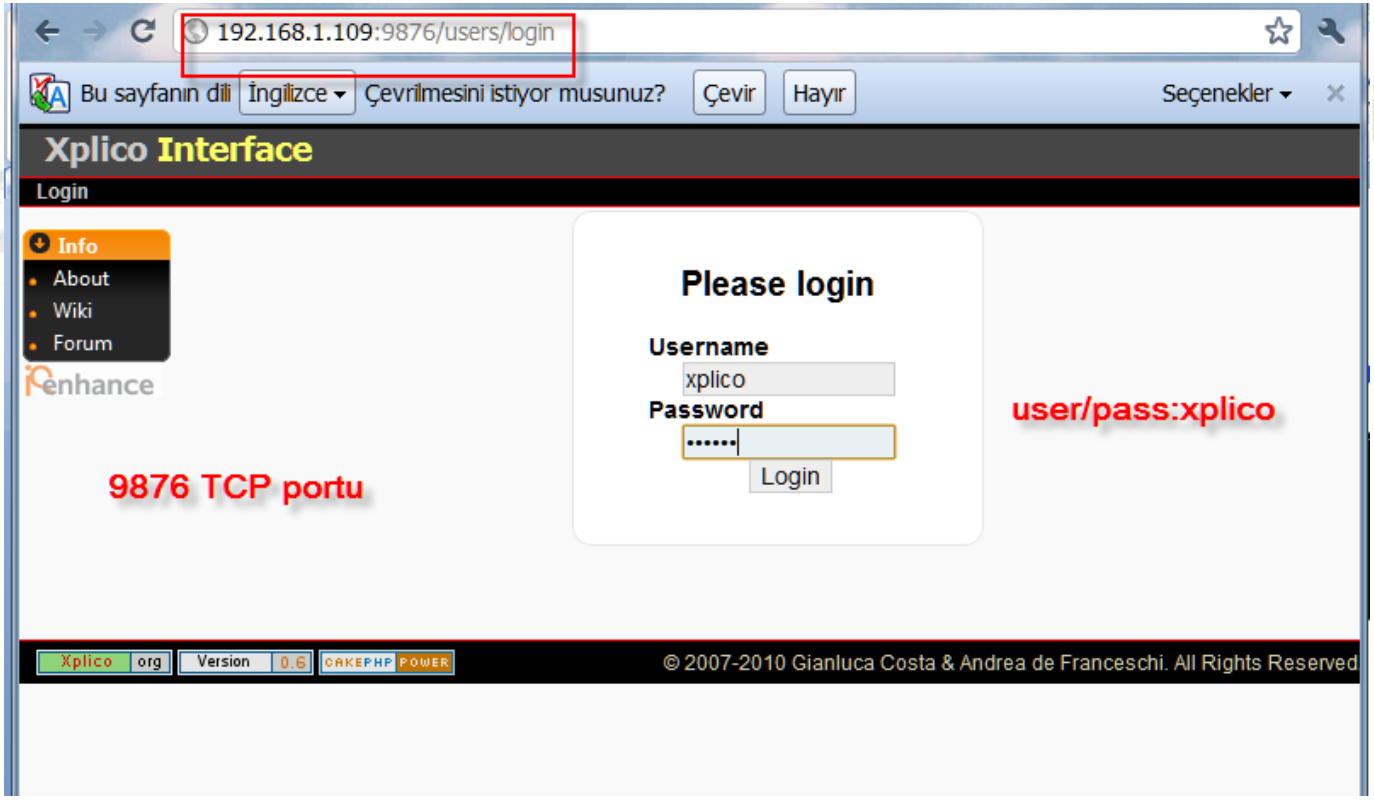
Dissector	Status	Note	Dissector	Status	Note
ARP	90%	—	PJL	90%	—
Radiotap	90%	—	NNTP	95%	—
Ethernet	100%	—	MSN	60%	v1 beta
PPP	90%	—	IRC	85%	—
VLAN	95%	—	YAHOO	0%	—
L2TP	70%	—	GTALK	0%	—
IPv4	98%	—	EMULE	0%	—
IPv6	98%	—	SSL/TLS	0%	with keys
TCP	95%	—	IPsec	0%	with keys
UDP	100%	—	802.11	60%	no encryp.
DNS	80%	—	LLC	60%	—
HTTP	100%	—	MMSE	95%	over HTTP
SMTP	95%	—	Linux cooked	95%	SLL
POP	95%	—	TFTP	90%	—
IMAP	95%	—	SNOOP	100%	Format
SIP	80%	—	PPPoE	90%	—
RTP	70%	—	Telnet	90%	—
RTCP	60%	—	WebMail	90%	—
SDP	70%	—	Paltalk Exp.	60%	—
FB chat	90%	—	Paltalk	90%	—
FTP	90%	—	NetBIOS	5%	Ses. Mes.
IPP	90%	—	SMB	0%	—

Web Mail

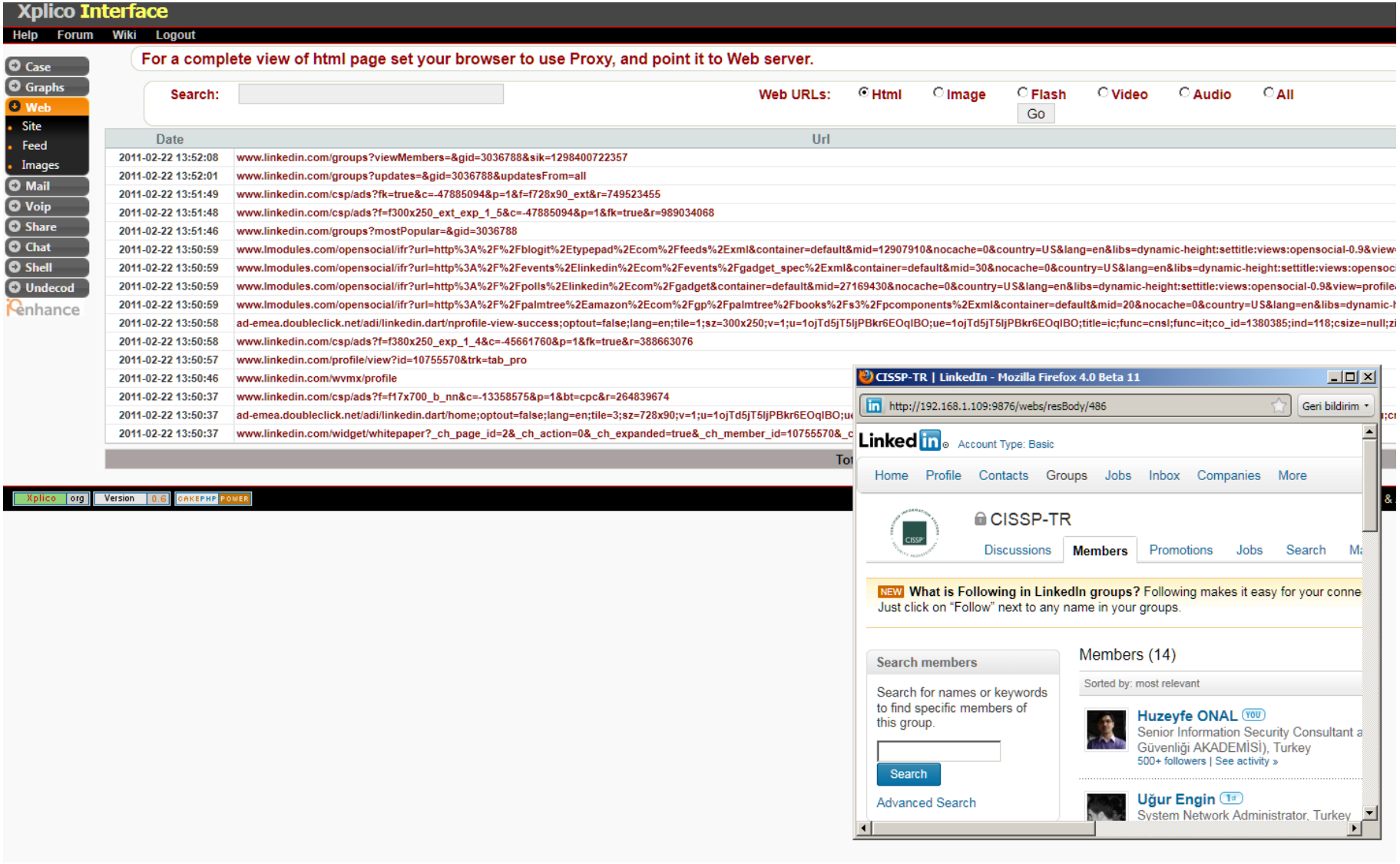
Yahoo!, AOL, Live

Xplico Kullanımı

```
#apache2ctl start

#service xplico start
```

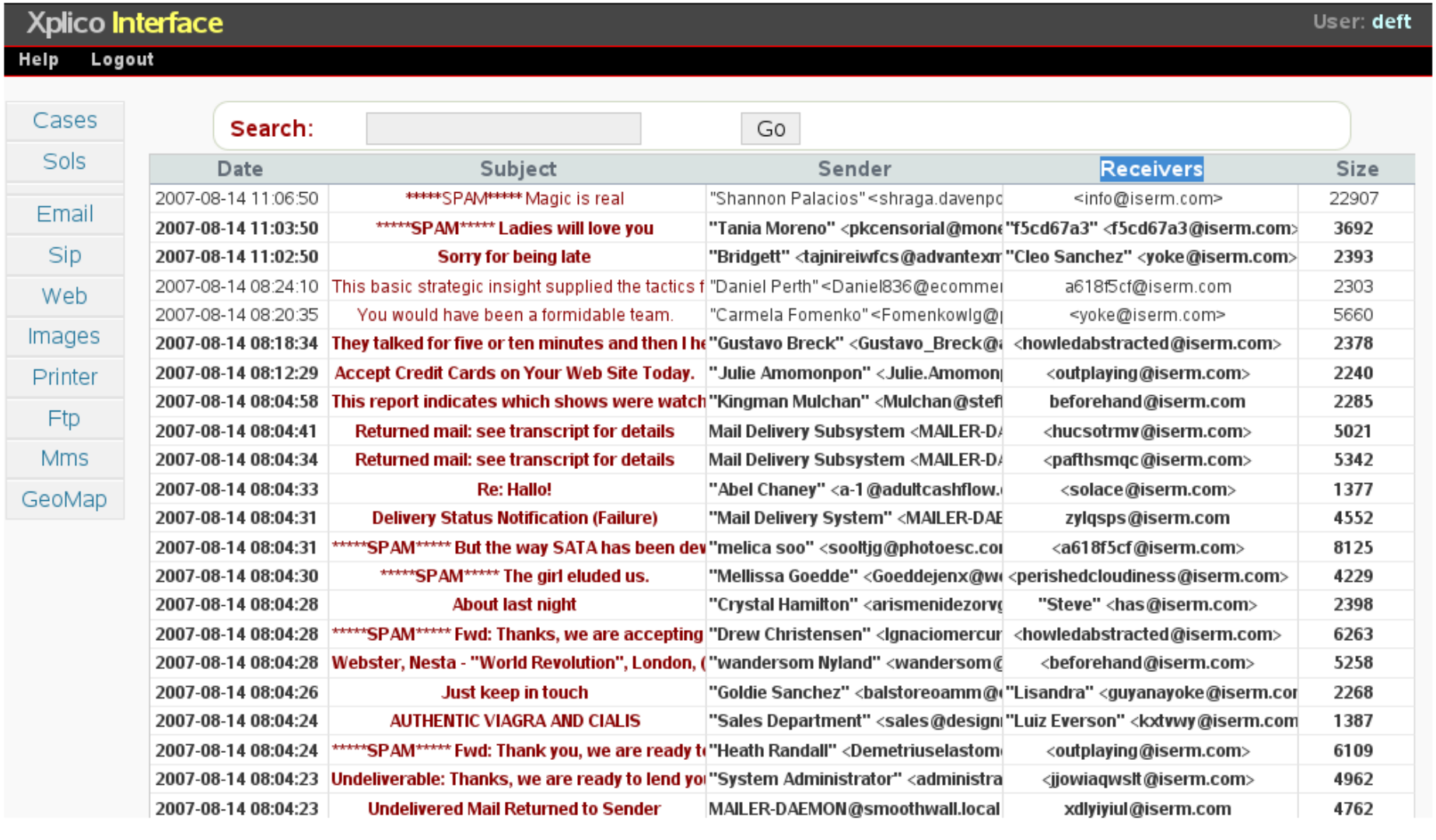


Web Gezinti Kaydı



Uygulama|Xplico ile Trafik Analizi

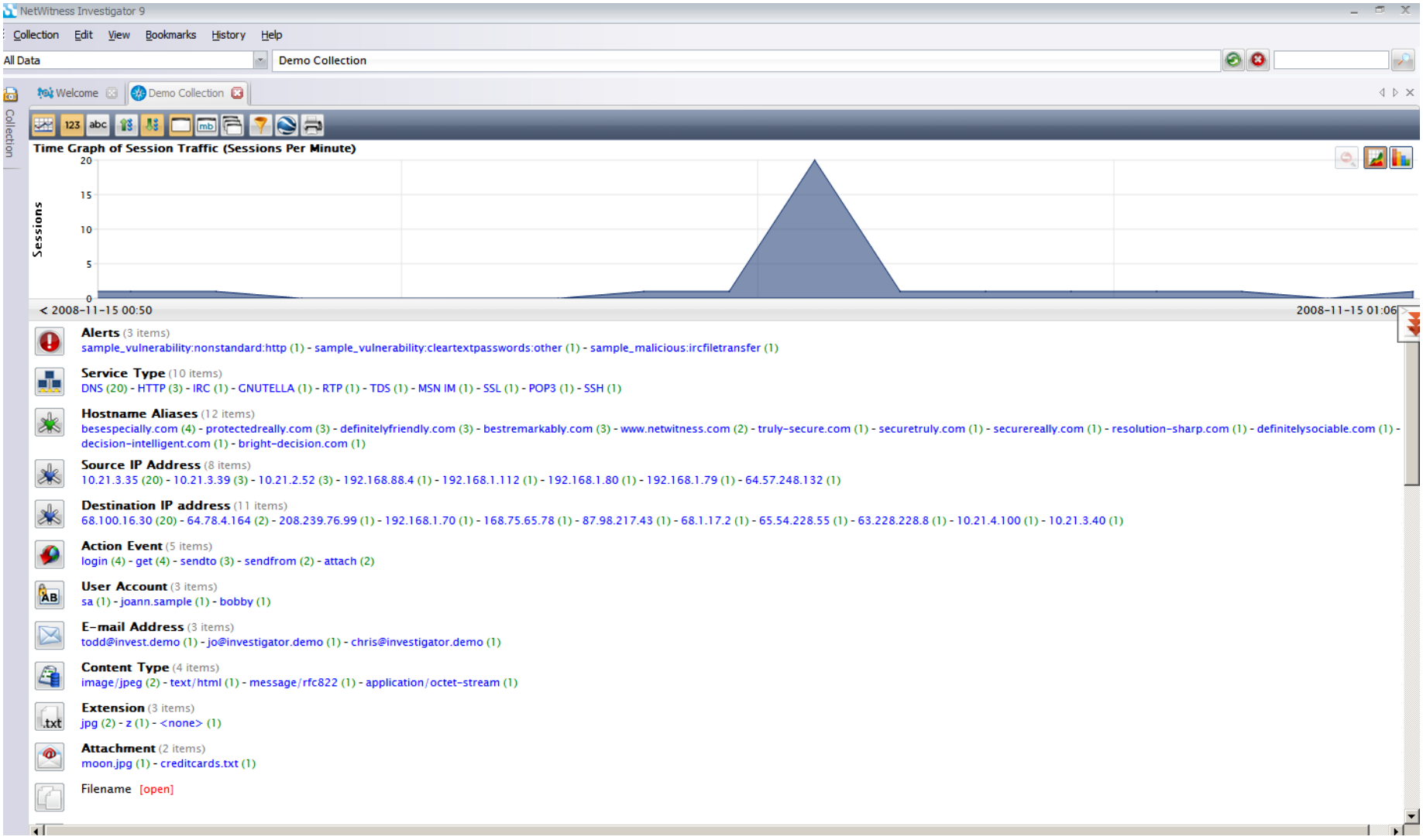
Xplico


Xplico Interface
User: deft
Help
Logout
Cases
Sols
Email
Sip
Web
Images
Printer
Ftp
Mms
GeoMap
Search:
Go
Date
Subject
Sender
Receivers
Size
2007-08-14 11:06:50 *****SPAM***** Magic is real "Shannon Palacios"<shraga.davenpc <info@iserm.com> 22907
2007-08-14 11:03:50 *****SPAM***** Ladies will love you "Tania Moreno" <pkcensorial@mone "f5cd67a3" <f5cd67a3@iserm.com> 3692
2007-08-14 11:02:50 Sorry for being late "Bridgett" <tajnireiwfcs@advantexm "Cleo Sanchez" <yoke@iserm.com> 2393
2007-08-14 08:24:10 This basic strategic insight supplied the tactics f "Daniel Perth"<Daniel836@ecommer a618f5cf@iserm.com 2303
2007-08-14 08:20:35 You would have been a formidable team. "Carmela Fomenko"<Fomenkowlg@ <yoke@iserm.com> 5660
2007-08-14 08:18:34 They talked for five or ten minutes and then I he "Gustavo Breck" <Gustavo_Breck@ <howledabstracted@iserm.com> 2378
2007-08-14 08:12:29 Accept Credit Cards on Your Web Site Today. "Julie Amomonpon" <Julie.Amomon <outplaying@iserm.com> 2240
2007-08-14 08:04:58 This report indicates which shows were watch "Kingman Mulchan" <Mulchan@stef beforehand@iserm.com 2285
2007-08-14 08:04:41 Returned mail: see transcript for details Mail Delivery Subsystem <MAILER-D <hucsotrmv@iserm.com> 5021
2007-08-14 08:04:34 Returned mail: see transcript for details Mail Delivery Subsystem <MAILER-D <pafthsmqc@iserm.com> 5342
2007-08-14 08:04:33 Re: Hallo! "Abel Chaney" <a-1@adultcashflow. <solace@iserm.com> 1377
2007-08-14 08:04:31 Delivery Status Notification (Failure) "Mail Delivery System" <MAILER-DAE zylqsps@iserm.com 4552
2007-08-14 08:04:31 *****SPAM***** But the way SATA has been dev "melica soo" <sooltjg@photoesc.co <a618f5cf@iserm.com> 8125
2007-08-14 08:04:30 *****SPAM***** The girl eluded us. "Mellissa Goedde" <Goeddejenx@w <perishedcloudiness@iserm.com> 4229
2007-08-14 08:04:28 About last night "Crystal Hamilton" <arismenidezorv "Steve" <has@iserm.com> 2398
2007-08-14 08:04:28 *****SPAM***** Fwd: Thanks, we are accepting "Drew Christensen" <Ignaciomercur <howledabstracted@iserm.com> 6263
2007-08-14 08:04:28 Webster, Nesta - "World Revolution", London, ("wandersom Nyland" <wandersom@ <beforehand@iserm.com> 5258
2007-08-14 08:04:26 Just keep in touch "Goldie Sanchez" <balstoreoamm@ "Lisandra" <guyanayoke@iserm.co 2268
2007-08-14 08:04:24 AUTHENTIC VIAGRA AND CIALIS "Sales Department" <sales@design "Luiz Everson" <kxtvwy@iserm.com 1387
2007-08-14 08:04:24 *****SPAM***** Fwd: Thank you, we are ready t "Heath Randall" <Demetriuselastom <outplaying@iserm.com> 6109
2007-08-14 08:04:23 Undeliverable: Thanks, we are ready to lend yo "System Administrator" <administra <jjowiaqwslt@iserm.com> 4962
2007-08-14 08:04:23 Undelivered Mail Returned to Sender MAILER-DAEMON@smoothwall.local xdlyiyiul@iserm.com 4762

Netwitness

- Ağ analiz ve network forensics çalışmalarının vazgeçilmez aracı,
- Ağ trafiği için “Google” işlevi görür,
- 2 GB kotaya kadar (pcap dosyası) ücretsiz kullanılabilir.

Netwitness


NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
Demo Collection
Welcome
Demo Collection
Time Graph of Session Traffic (Sessions Per Minute)
Sessions
20
15
10
5
0
< 2008-11-15 00:50
2008-11-15 01:06
Alerts (3 items)
sample_vulnerability:nonstandard:http (1) - sample_vulnerability:cleartextpasswords:other (1) - sample_malicious:ircfiletransfer (1)
Service Type (10 items)
DNS (20) - HTTP (3) - IRC (1) - GNUTELLA (1) - RTP (1) - TDS (1) - MSN IM (1) - SSL (1) - POP3 (1) - SSH (1)
Hostname Aliases (12 items)
besespecially.com (4) - protectedreally.com (3) - definitelyfriendly.com (3) - bestremarkably.com (3) - www.netwitness.com (2) - truly-secure.com (1) - securetruly.com (1) - securereally.com (1) - resolution-sharp.com (1) - definitelysociable.com (1) - decision-intelligent.com (1) - bright-decision.com (1)
Source IP Address (8 items)
10.21.3.35 (20) - 10.21.3.39 (3) - 10.21.2.52 (3) - 192.168.88.4 (1) - 192.168.1.112 (1) - 192.168.1.80 (1) - 192.168.1.79 (1) - 64.57.248.132 (1)
Destination IP address (11 items)
68.100.16.30 (20) - 64.78.4.164 (2) - 208.239.76.99 (1) - 192.168.1.70 (1) - 168.75.65.78 (1) - 87.98.217.43 (1) - 68.1.17.2 (1) - 65.54.228.55 (1) - 63.228.228.8 (1) - 10.21.4.100 (1) - 10.21.3.40 (1)
Action Event (5 items)
login (4) - get (4) - sendto (3) - sendfrom (2) - attach (2)
User Account (3 items)
sa (1) - joann.sample (1) - bobby (1)
E-mail Address (3 items)
todd@invest.demo (1) - jo@investigator.demo (1) - chris@investigator.demo (1)
Content Type (4 items)
image/jpeg (2) - text/html (1) - message/rfc822 (1) - application/octet-stream (1)
Extension (3 items)
jpg (2) - z (1) - <none> (1)
Attachment (2 items)
moon.jpg (1) - creditcards.txt (1)
Filename [open]

Ağ Trafiğinde Bilgi Arama

- Akan trafikte veya kaydedilmiş trafik dosyaları üzerinde işlem yaparken trafik içerisinde belirli bilgileri bulma amacıyla kullanılır.
  - X, Y zamanında kimlere e-posta göndermiş?
  - Trafikte fenerbahçe kelimesini kullananların raporu

Grep

- Grep: UNIX/Linux sistemlerde dosya içerisinde belirli düzene uyan stringlerin/satırların bulunmasını sağlar.
  - UNIX/Linux sistemlerin Google'u
  - Google'dan önce grep vardı
- #grep huzeyfe /etc/passwd
- #grep –R huzeyfe *.php
- #grep –v huzeyfe /etc/passwd
- #grep ^GET /etc/TEST
- #grep –i http /etc/passwd

Network Grep:Ngrep

- Ngrep(Network Grep): grep benzeri bir yazılım fakat klasik dosyalarda değil de ağ trafiğinde arama/bulma işlemi yapar.
- Network DLP ve IDS(Intrusion Detection System) yazılımlarının atası sayılabilir.
- Ascii ve hex türünde arama yapabilir.
- Canlı ağ trafiğinde veya kaydedilmiş ağ trafiği içerisinde arama işlemi gerçekleştirebilir.
- Örnek: Tüm ağ trafiği içerisinde huzeyfe geçen paketleri ekrana bas
  - #ngrep –q huzeyfe –d eth0

Ngrep ile Ne Yapılabilir?

- Ağ içerisinde geçen özel bir kelime arattırılabilir.
- IDS'lere imza yazmak için kullanılabilir.
- Protokol anormallikleri yakalanabilir.
  - Http portu üzerinden kullanılan SSH bağlantılarını ngrep ile keşfedebilirsiniz.
  - Port/protokol tünelleme programlarını ortamda hiçbir IPS, Firewall vs ye ihtiyaç duymadan Ngrep ile yakalanabilir.
- Ağda şifresiz protokolleri kullananların gizli biglileri yakalanabilir.

Ngrep ile SMTP Analizi

```
[root@mail ~]# ngrep -q -i 'rcpt to:|mail from:' tcp port 25
interface: rl0 (111.111.111.11/255.255.255.248)
filter: (ip or ip6) and ( tcp port 25 )
match: rcpt to:|mail from:
T 213.154.215.92:4257  -> 80.93.212.86:25  [AP]
  MAIL FROM: <soonmantse@barbara.com>..RCPT TO: <robertgray@asninvest.ru>..DATA..
T 87.212.128.168:1284  -> 80.93.212.86:25  [AP]
  RCPT TO: <rich_vip@asninvest.ru>..
T 77.123.113.49:14892  -> 80.93.212.86:25  [AP]
  MAIL FROM: <sphsophie@hotmail.com>..RCPT TO: <salat-afonya@asninvest.ru>..DATA..
```

Http portundan yapılan ssh

- HTTP portundan neden SSH yapılır?

```
# ngrep -q -i SSH tcp port 80
interface: r10 (111.111.111.11/255.255.255.248)
filter: (ip or ip6) and ( tcp port 80 )
match: SSH

T 80.93.212.86:80 -> 212.252.168.235:44020 [AP]
  SSH-2.0-OpenSSH_4.5p1 FreeBSD-20061110.
T 80.93.212.86:80 -> 212.252.168.235:44034 [AP]
  SSH-2.0-OpenSSH_4.5p1 FreeBSD-20061110.
T 212.252.168.235:44034 -> 80.93.212.86:80 [AP]
  SSH-2.0-OpenSSH_5.0.
T 80.93.212.86:80 -> 212.252.168.235:44034 [AP]
  .......^...D.....=z......~diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman
```

```
# ngrep -q -i '^SSH' tcp

T 80.93.212.86:443 -> 212.252.168.235:44197 [AP]
  SSH-2.0-OpenSSH_4.5p1 FreeBSD-20061110.

T 212.252.168.235:44197 -> 80.93.212.86:443 [AP]
  SSH-2.0-OpenSSH_5.0.
```

- Bu komutu biraz daha geliştirip SSH portu harici herhangi bir porttan SSH kullanmaya çalışanları izleyebilirsiniz.
  - Ngrep –q –i ‘^SSH’ not tcp port 22

Ngrep'i IDS Olarak Kullanma

- Amaç: HTTP portu üzerinden yapılan fakat http olmayan bağlantıları izleme:

```
#ngrep -q -W byline -v '^GET|POST|PUT|HTTP/1.[01]' tcp port 80

filter: (ip or ip6) and ( tcp port 80 and dst host 80.93.212.86 )
don't match: ^GET|POST|PUT|HTTP/1.[01]
T 212.252.168.253:23885 -> 80.93.212.86:80 [AP]
SSH-2.
```

Ngrep Kısıtlamaları

- Ngrep ve şifreli protokoller
  - Ngrep normalde şifreli protokolleri inceleyemez.
  - İnceleyebilmesi için şifreli protokollerin bir şekilde deşifre edilmesi gerekir.
- Parçalanmış Paketler ve Ngrep
  - Doğası gereği Ngrep her gelen paketi ayrı değerlendirir ve parçalanmış paketleri anlamaz ve yazacağınız düzenli ifadeler fragmented paketlerde işe yaramaz.
- Yüksek trafik
  - Ngrep yüksek bantgenişliğne sahip ağlarda paket kaybına sebep olabilir ve yakalama işlemlerini sağlıklı gerçekleştiremez.

Ağ Tabanlı IDS/IPS Sistemleri

Tanımlar:Saldırı Tespit Sistemi

- IDS – Intrusion Detection System
  - Saldırı Gözlem Sistemleri
  - Gerçek dünya örneği: Arabalara takılan alarm
- Günümüzde daha çok pasif bilgi toplama amaçlı kullanılmaktadır.
- Dikkatli kullanılmazsa

İşe yaramaz(gereksiz alarmlar)

Tanımlar:Saldırı Engelleme Sistemi

- IPS – Intrusion Protection System
  - Saldırı Gözlem ve Engelleme Sistemleri
  - Elektrik verilmiş dikenli tel ☺
- Aktif sistemlerdir, hata kabul etmez!
- Günümüzde çoğu şirkette nazar boncuğu işlevi görürler
- Neden?

Saldırı Tespiti

- İlk adım: Saldırı tanımını belirleme
- İkinci adım: Bu tanıma uyan hareketlerin IDS dilinde tanımlanması
- Üçüncü adım:Saldırı Tespit Sisteminin uygun konumda çalıştırılması ve çıktılarının yorumlanması

Saldırı Tespit Yöntemleri

- **Saldırıyı nasıl tespit edebiliriz?**
  - İmza tabanlı saldırı tespiti
  - Kural tabanlı saldırı tespiti
  - Protokol anormalliği aracılığıyla saldırı tespiti
  - Trafik anormallik tespit yöntemi aracılığıyla
  - Log izleme aracılığıyla

Protokol Anormalliği Tespiti-I

- İç ağdan dışarı Tünelleme Yazılımı kullananların belirlenmesi
- Eldeki veriler:
  - Şirket güvenlik politikasına göre kullanıcıların sadece 80 ve 443. portlardan internete erişimi vardır.
  - Tünelleme yapılıyorsa bu iki porttan yapılmalı.
  - HTTP ve HTTPS protokollerinin detay yapıları.

Protokol Anormalliği Tespiti-II

- Tehditi günlük konuşma dilinde belirleme
  - 80. porttan HTTP harici herhangi bir protokol geçiyorsa bir anormallik (tünelleme?) vardır
- IDS mantığına uyarlarsak:
  - 80.portta HTTP protokolüne ait olan komutlar dışında bir trafik görürsen uyarı ver!

```
#ngrep -q -W byline -v '^GET|POST|PUT|HTTP/1.[01]' tcp port 80

filter: (ip or ip6) and ( tcp port 80 and dst host 80.93.212.86 )
don't match: ^GET|POST|PUT|HTTP/1.[01]
T 212.252.168.253:23885 -> 80.93.212.86:80 [AP]
SSH-2.
```

IDS/IPS Çeşitleri

- Ağ Tabanlı IDS/IPS Sistemleri
  - Snort, TippingPoint, Mcafee, IBM ISS Proventia
- Kablosuz Ağ Saldırı Tespit Sistemleri
  - Kismet
- Host Tabanlı IDS/IPS Sistemleri
  - Mcafee HIPS
- Log Tabanlı IDS/IPS Sistemleri
  - Ossec
- Dosya Bütünlük İzleme Sistemler
  - Kritik dosyaların erişim, içerik ve haklarındaki değişiklikler
  - Tripwire, Osiris

Ağ Tabanlı Integrity Checking

- DNS, whois, site içeriği, karalistelere girme durumu, SSL sertifika durumu gibi bilgilerin değişip değişmediğini 7X24 kontrol eden ve ve değişiklik anında size haber vermesini sağlayan sistemdir.

Kablosuz Ağ Saldırı Tespit Sistemleri

- Wireless IDS/IPS
- Kablosuz ağa izinsiz girişleri engelleme amaçlı
- Basit çalışma mantığı
  - Ağda tanımlı MAC adreslerini ve AP isimlerini al
  - Çecrede bunlardan başka bağlantı yapmak isteyenlere Deauth paketleri gönder, logla
- Kismet kullanılarak yapılabilir.

Ağ Tabanlı IDS/IPS Sistemleri

- Sınır güvenliğinde en etkin bileşen
- Ağ trafiği üzerinde işlem yapar, tüm ağı korur
- Dedike bir donanım gerektirir.
- L2'den L7'e kadar tüm katmanlarda protokol incelemesi yapabilir.

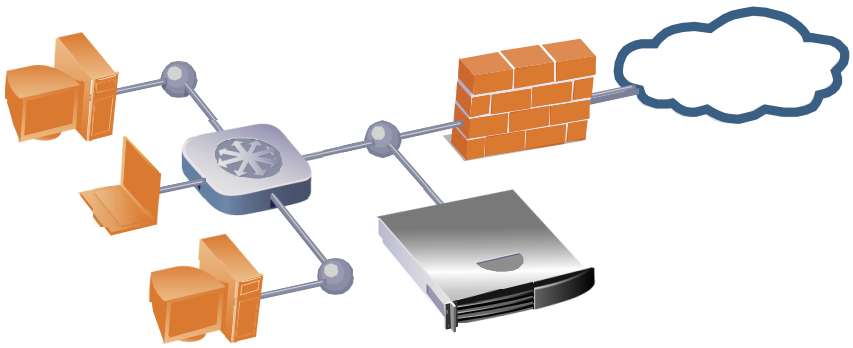
Firewall – IPS Farkı

Firewall(Güvenlik Duvarı)	IPS(Saldırı Engelleme Sistemi)
• OSI'de 4. katmana kadar iş yapar(MAC-IP-PORT) • Paket başlıklarıyla ilgilenir • Zaman süreli engelleme özelliği yoktur(genelde) • Kuralları basittir, esnemez!	• OSI'de 2-7 arası tüm katmanlarda iş yapar • Paket başlık ve payload(veri)ile ilgilenir • Zaman süreli engelleme özelliği vardır(beş dakika gibi) • Kuralları karışıktır, istenildiği gibi esnetilebilir

(Network)IDS/(Network)IPS Farkı

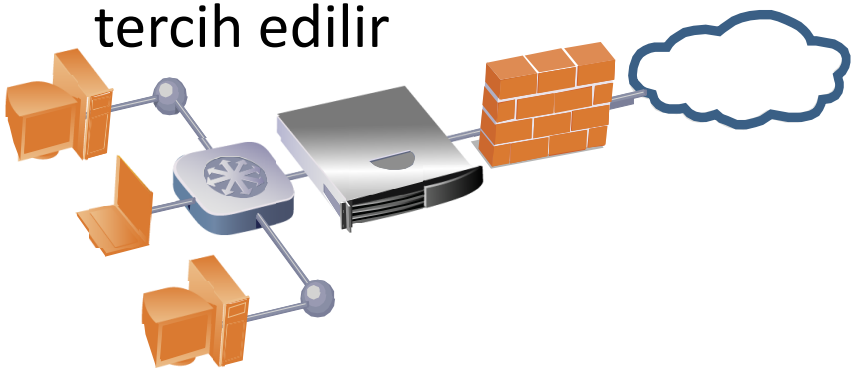
IDS(Saldırı Tespit Sistemi)

- ‘90ların başı
- False positive olabilir
- False negative olabilir
- İzleme Amaçlı
- Her yerde kullanılabilir



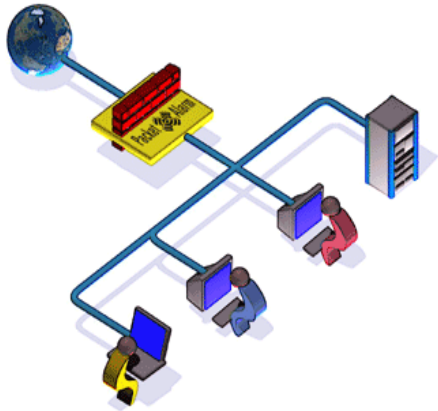
IPS(Saldırı Engelleme Sistemi)

- 2000’lerin başı
- False positive olmamalı
- False negative olmamalı
- Engelleme Amaçlı
- Daha çok sınır güvenliğinde tercih edilir



IPS Yerleşimi

- IPS kullanımında en önemli konu!
- Ağın durumuna göre yerleşim önemli
- Switch Span portu, özel network tap cihazları(Internal)
  - Linux/BSD yüklü sağlam sunucu
- Fail Open, Fail Close Özelliği
  - IPS modunda (Inline) mutlaka bypass modülü olmalı

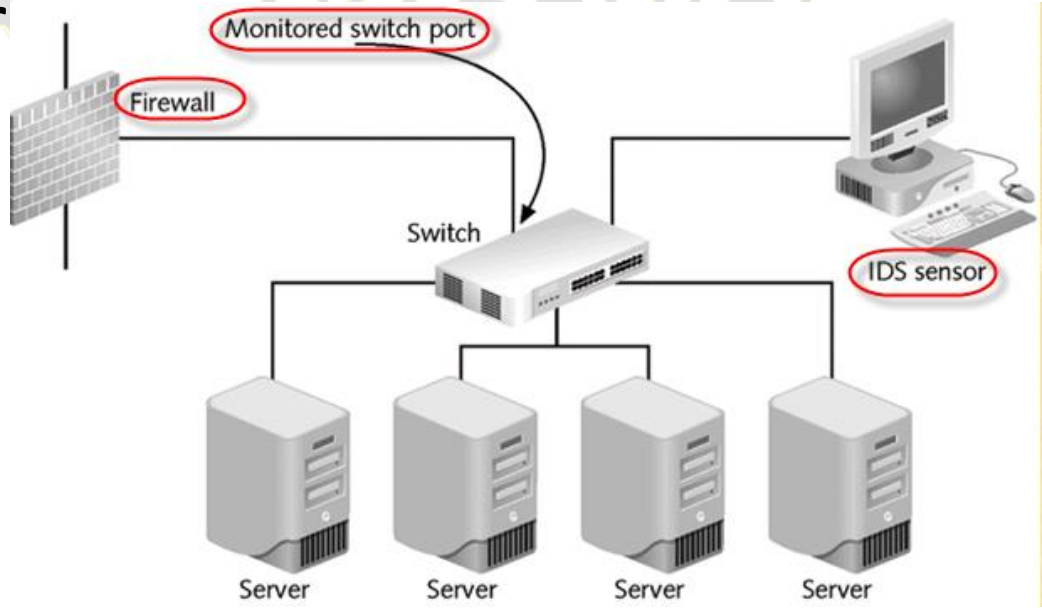


IPS Yerleşimi

Firewall Önü	Firewall Arkası
• Yüklü miktarda uyarı, gereksiz trafik • Tehditleri daha iyi belirler • Gereksinim olabilir(birden fazla Firewall vs) • SSL şifreleme çözemez(?)	• Sadece FW'an geçen paketler, trafik yoğunluğu az • Tehditleri daha az ama daha gerçek(false positive oranı çok düşük)belirleyebilir. • SSL Şifreleme Çözebilir(?)

IDS Yerleşimi

- İncelenmesi istenen trafiğin tamamını görebilecek bir noktaya yerleştirilmeli
- Switch Span portu, özel network tap cihazları(Internal)
- Dağıtık yapıda olabilir



Snort IPS Kullanımı

Snort'un desteklediği, kullanılabilir özellikler

Efektif Snort kullanımı

Snort Hakkında Yanlış Bilinenler

- Snort performanslı değildir!
  - Snort=mysql+text loglama+snort+....
- Snort saldırıları engelleyemez, sadece uyarı verir
- Snort DDoS saldırılarını engeller
- Snort DDoS saldırılarını engelleyer
- Snort'da false positive çoktur
- Snort protokolleri tanıyamaz
- Snort ticari desteği yoktur!

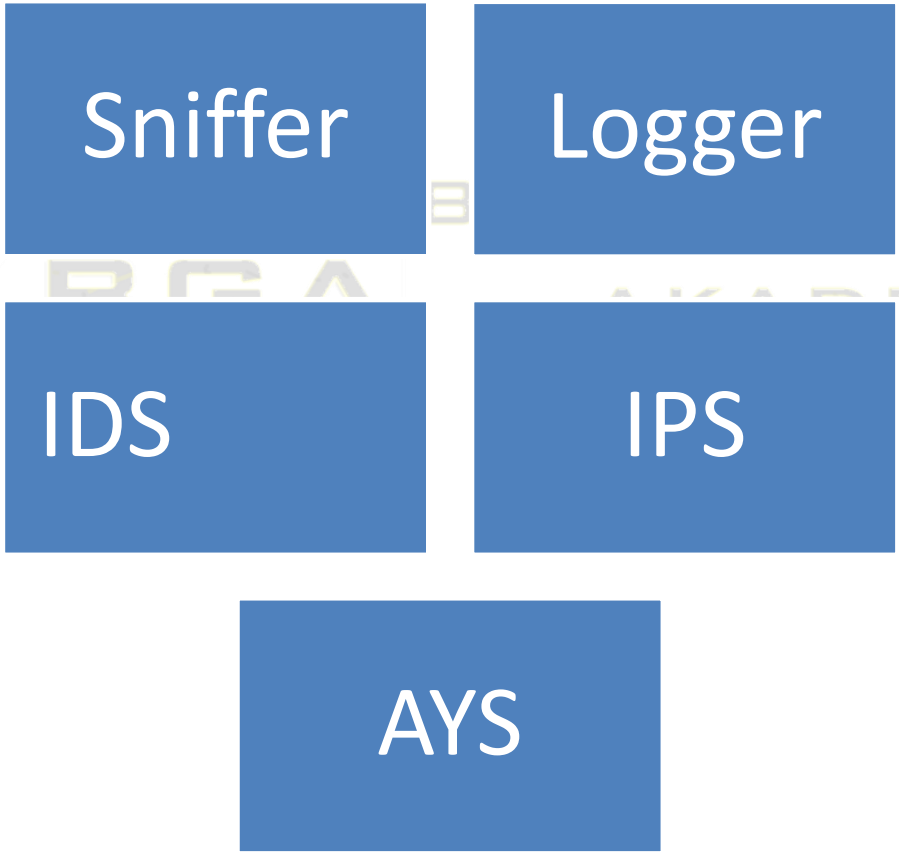
Snort: Açık Kod IPS Sistemi

- Snort 3.5~ milyon indirme sayısıyla dünyada en fazla tercih edilen açık kaynak kodlu IDS/IPS yazılımıdır.
- Açık Kaynak Kodlu, Özgür Lisansa Sahip
- ’98 yılında hobi amaçlı başlangıç
- Günümüzde: akademik, askeri, ticari kullanım alanları
- Linux/UNIX/Windows
- Stateful Packet Tracking
- Hedef tabanlı IDS özelliği
- Ipv6 desteği
- Firewall’lara komut gönderimi
- Esnek kural dili

Kullanım Alanları

- Snort çeşitli kullanım alanlarına sahiptir.
  - Sniffer
  - NIDS (Ağ Tabanlı Saldırı Tespit Sistemi)mod
  - NIPS(Ağ Tabanlı Saldırı Engelleme) mod
  - Anormallik Tespit Sistemi
  - DDOS Engelleme Sistemi
  - NFA(Network Forensic Analys) Aracı
  - DLP(Veri Sızma Kontrolü)

Snort Çalışma Modları



Snort:Sniffer Mod

- TCP/IP başlık bilgilerini yakalama amaçlı kullanılır(Sniffer->tcpdump)
- TCP/UDP/ICMP başlık bilgilerini yakalama için
  - #snort –v
- L2 başlık bilgilerini yakalama için
  - #snort –ve
- Pakelerdeki veri kısmını(payload) yakalama için
  - #snort -vde

Sniffer Mod Detayları

#snort –v –d –i emo tcp port 80

04/12-20:15:13.213759 79.230.231.214:2678 -> 212.98.228.246:80 TCP TTL:107 TOS:0x0 ID:25922 IpLen:20 DgmLen:1032 DF ***AP*** Seq: 0x906935F8 Ack: 0x4775C2C7 Win: 0xFAD4 TcpLen: 20
47 45 54 20 2F 43 6F 6D 70 6F 6E 65 6E 74 73 2F GET /Components/

04/12-20:15:13.213759

Zaman damgası

79.230.231.214:2678

Kaynak IP:Kaynak Port

6E 65 6E 74 73 2F GET /Components/

Payload(Veri Alanı)

TCP TTL:107 TOS:0x0

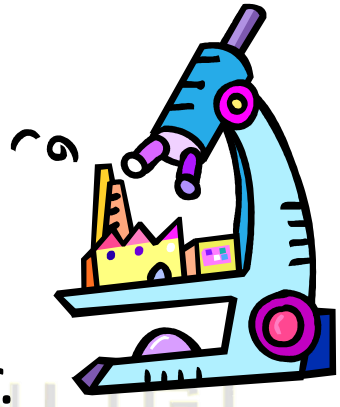
TCP detayları

212.98.228.246:80

Kaynak IP:Kaynak Port

Snort:Paket Kaydedici Mod

- Yakalanan paketleri diske kaydetme için kullanılır.
  - #snort –l /var/log/snort
  - -l logların h angi dizine kaydedileceğini belirler.
  - Loglar /var/snort/log dizininde IP adresine göre kayıt edilecektir.
  - -b eklenirse loglar binary formatta(pcap) kaydedilir. Özellikle yoğun ağlarda tercih edilmeli.

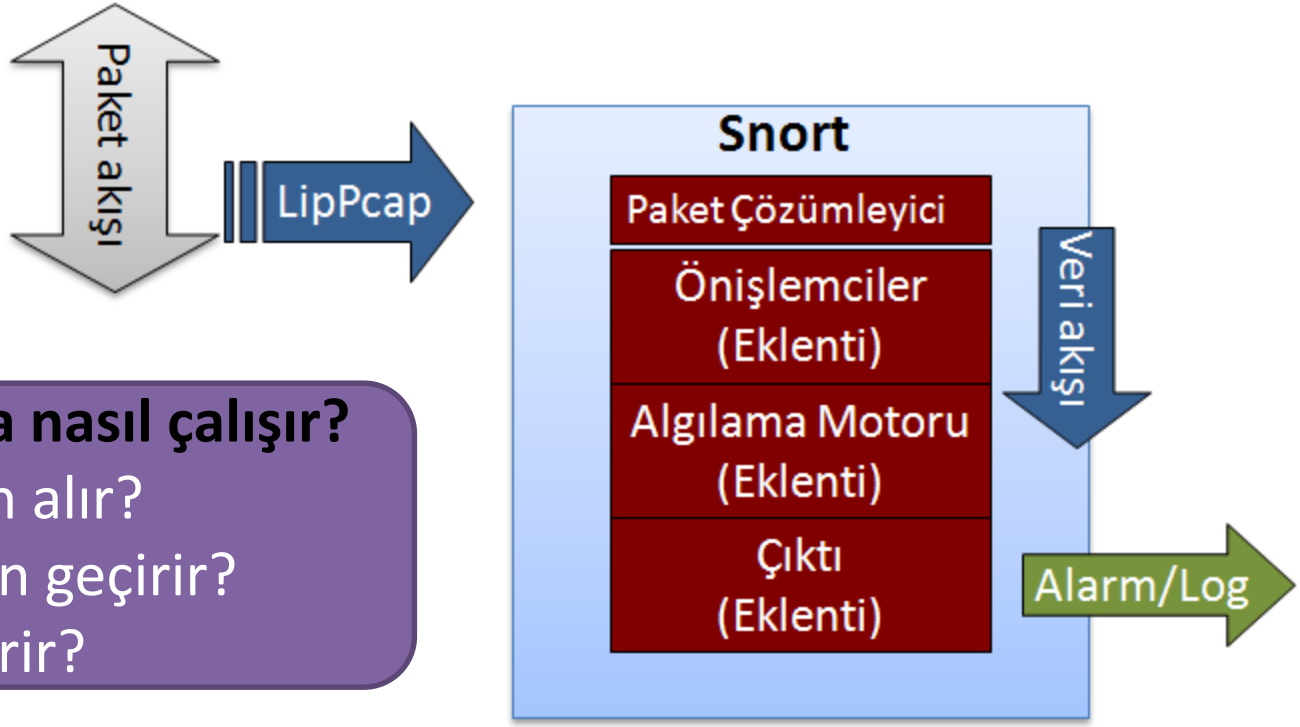


```
[root@vps-fw /var/log/snort]# ls -ltr
total 87212
-rw-------  1 root  wheel       279 May 14 02:15 snort.log.1242256339
-rw-------  1 root  wheel   2914430 May 14 23:24 snort.log.1242256533
-rw-------  1 root  wheel   3243911 May 14 23:48 snort.log.1242332799
-rw-------  1 root  wheel       859 May 14 23:51 snort.log.1242334261
-rw-------  1 root  wheel       189 May 14 23:52 snort.log.1242334338
-rw-------  1 root  wheel     68502 May 14 23:55 snort.log.1242334375
-rw-------  1 root  wheel     33617 May 15 00:03 snort.log.1242334622
-rw-------  1 root  wheel  70803538 May 16 10:30 snort.log.1242335026
-rw-------  1 root  wheel  12098645 May 16 10:30 alert
```

Snort:NIDS Mod

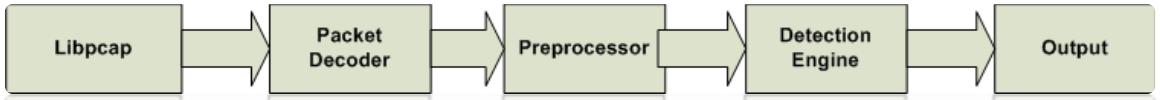
- Yakalanan trafik içerisinde saldırı imzası aranır.
- Bu modda performans çok önemlidir. Gereksiz parametrelerden kaçınılmalı
- #snort –l /var/log/snort –c /etc/snort/snort.conf –d –i eth0
  - eth0 arabirimi üzerinden yakalanan trafik eğer snort.conf'a uyuyorsa bu paketleri veri kısımlarıyla birlikte log dizinine kaydet.
  - Bu haliyle paketler ascii kaydedilecektir. –b parametresi ile paketlerin binary kaydedilmesi sağlanabilir.

Snort NIDS Mod İnceleme

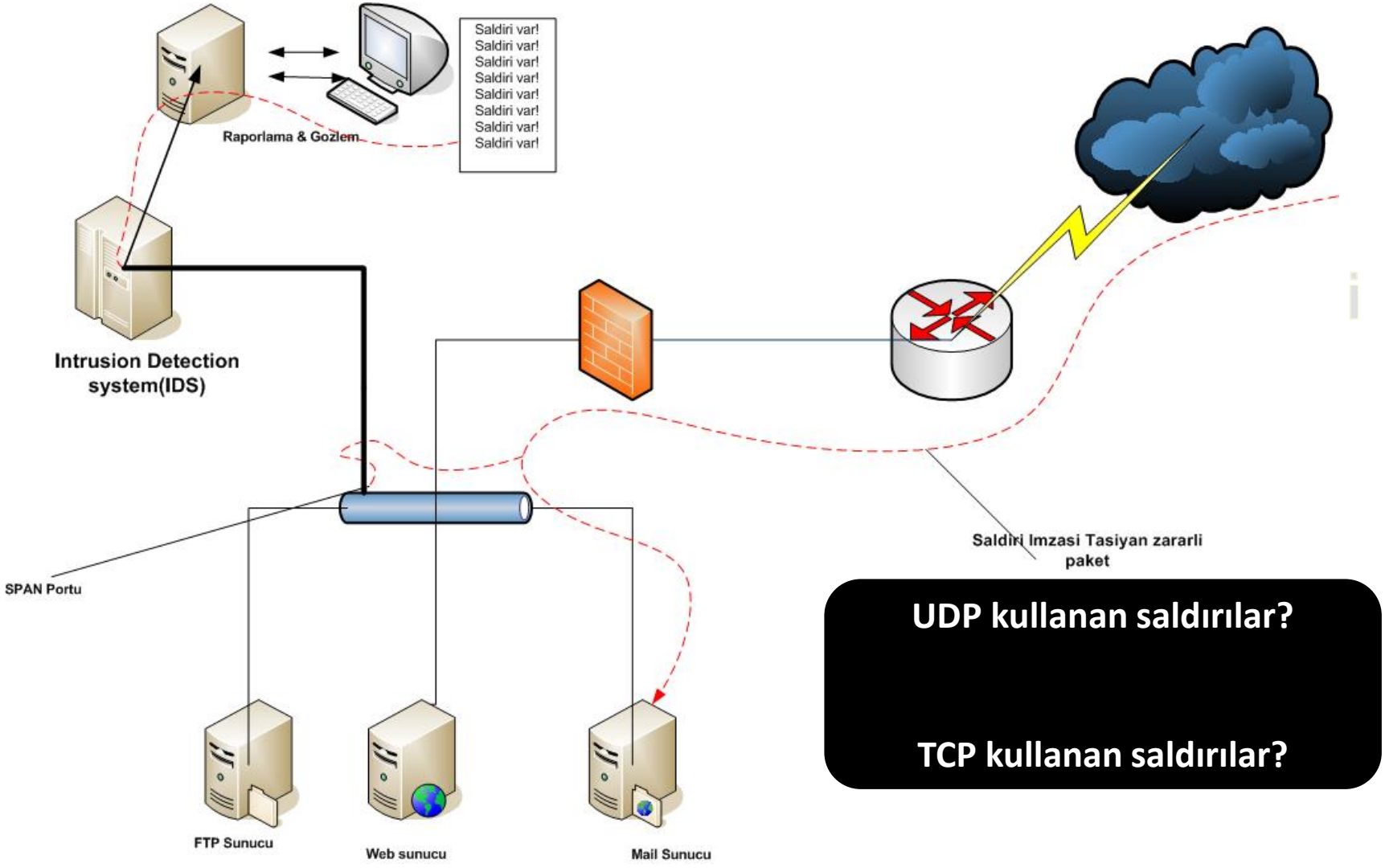


Snort IDS modda nasıl çalışır?

- Paketleri nerden alır?
- Hani süreçlerden geçirir?
- Nasıl bir çıktı verir?



NIDS Mod Detaylar

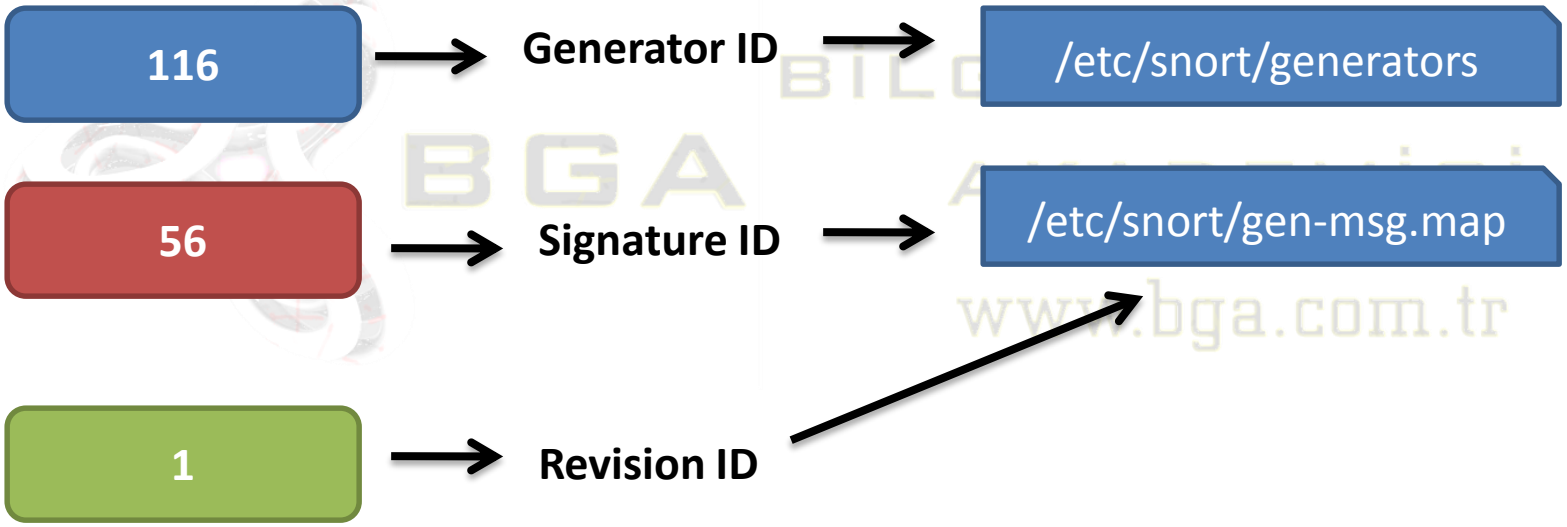


UDP kullanan saldırılar?

TCP kullanan saldırılar?

Örnek Alarm Kaydı

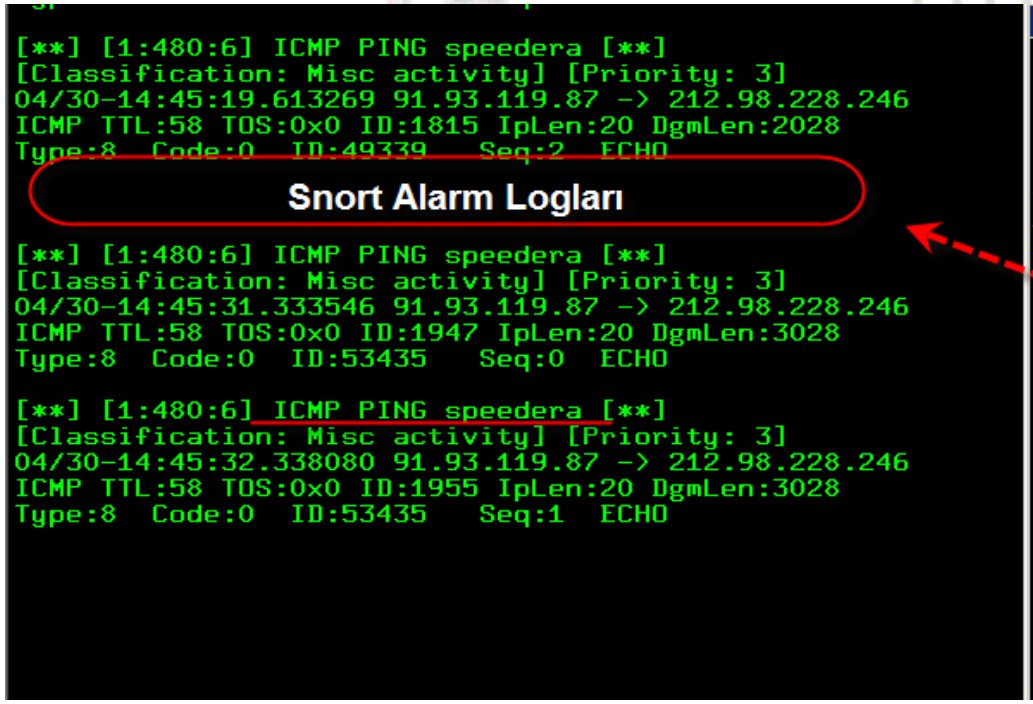
```
[**] [116:56:1] (snort_decoder): T/TCP Detected [**]
```

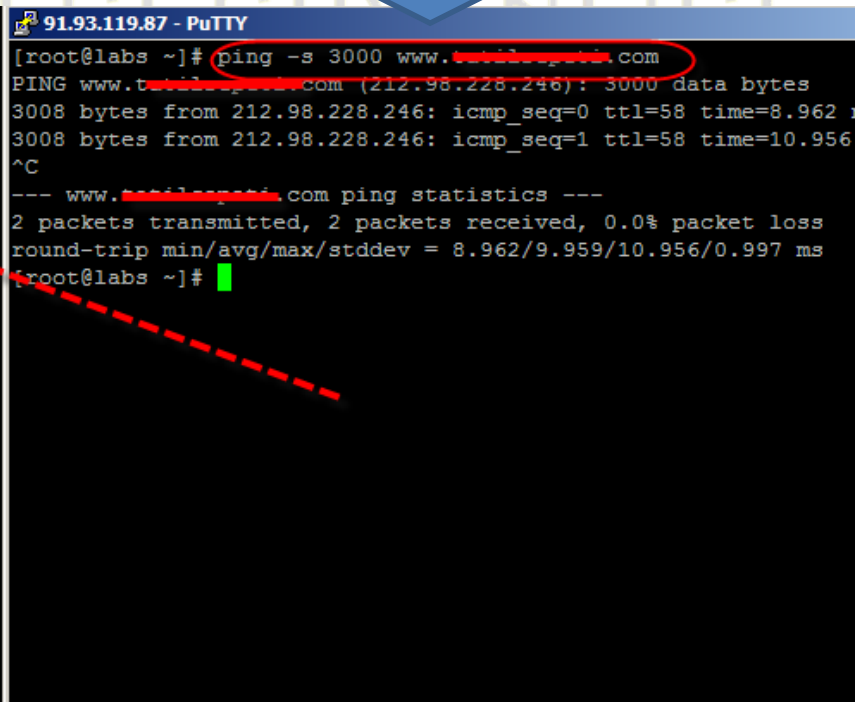


Snort (N)IDS Örnek

Trafiği pasif olarak izleyip anormal paketlere(anormal paketler imzalarda tanımlanmış olmalı) uyarı verir

3000 byte ICMP paketi gönderiliyor

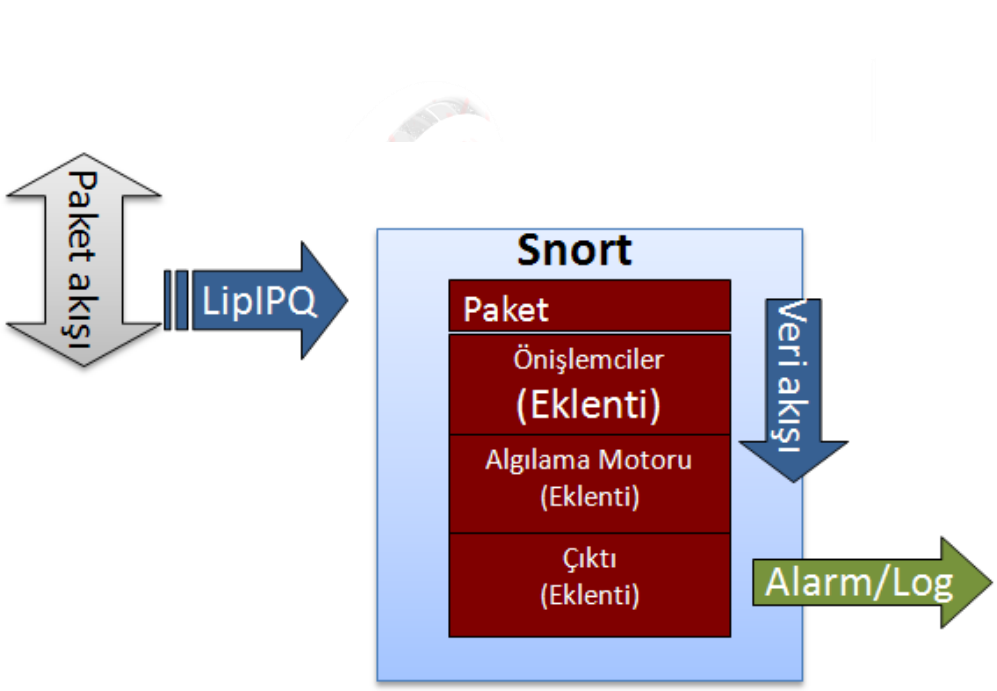


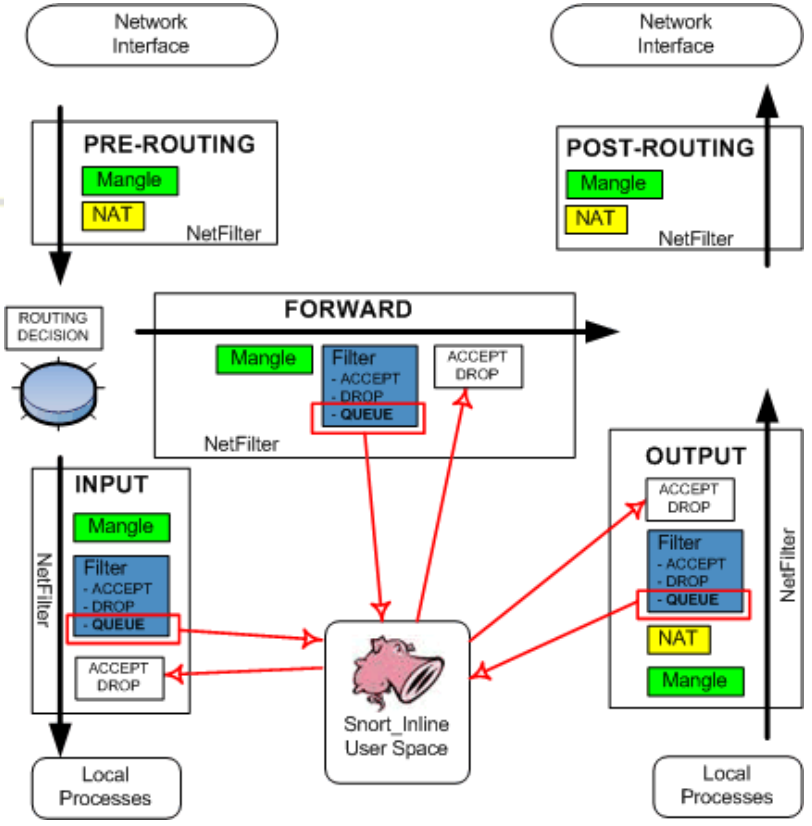


Snort:NIPS Mod

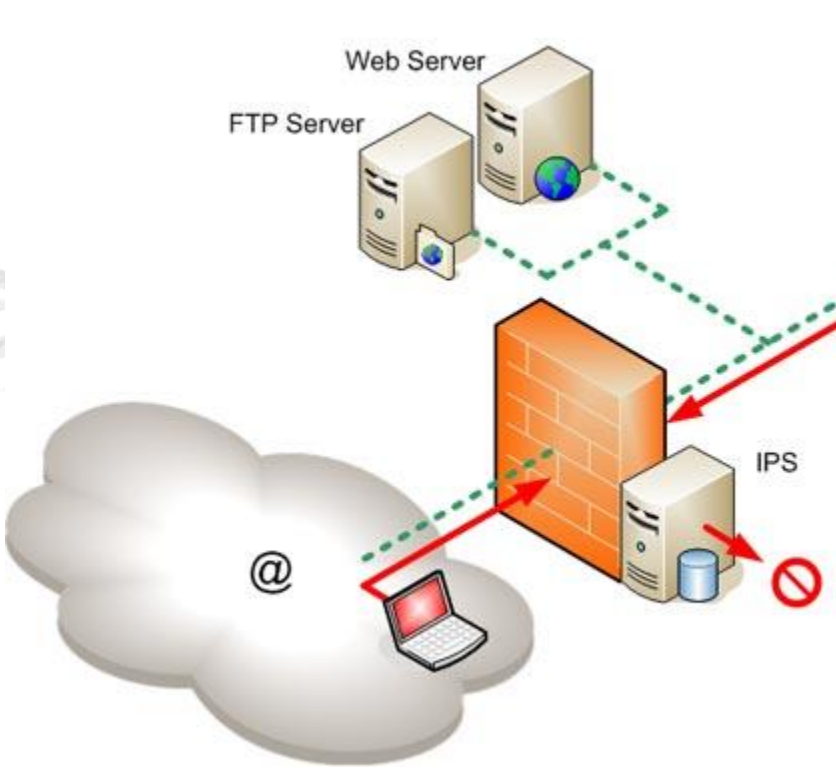
- Saldırı engelleme modu(Inline mod olarak da geçer)
- NIDS modu paketleri libpcap üzerinden alır
- NIPS modu paketleri libipq üzerinden alır, paketin içeriğine göre iptables'la engelleme ya da izin verme işlemi yapar.
- Inline modda üç çeşit kural vardır:
  - Drop: paketi engelle ve Snort ile logla
  - Reject:paketi engelle ve TCP RST dön
  - Sdrop: paketi engelle ve loglama

Snort NIPS Mod İnceleme





NIPS Mod Yerleşim Planı



- Inline yerleşim şart!
- Cihaz L2(bridge mod) veya L3 çalışabilir.
- En sağlıklı çözüm

NIPS Modda Engelleme

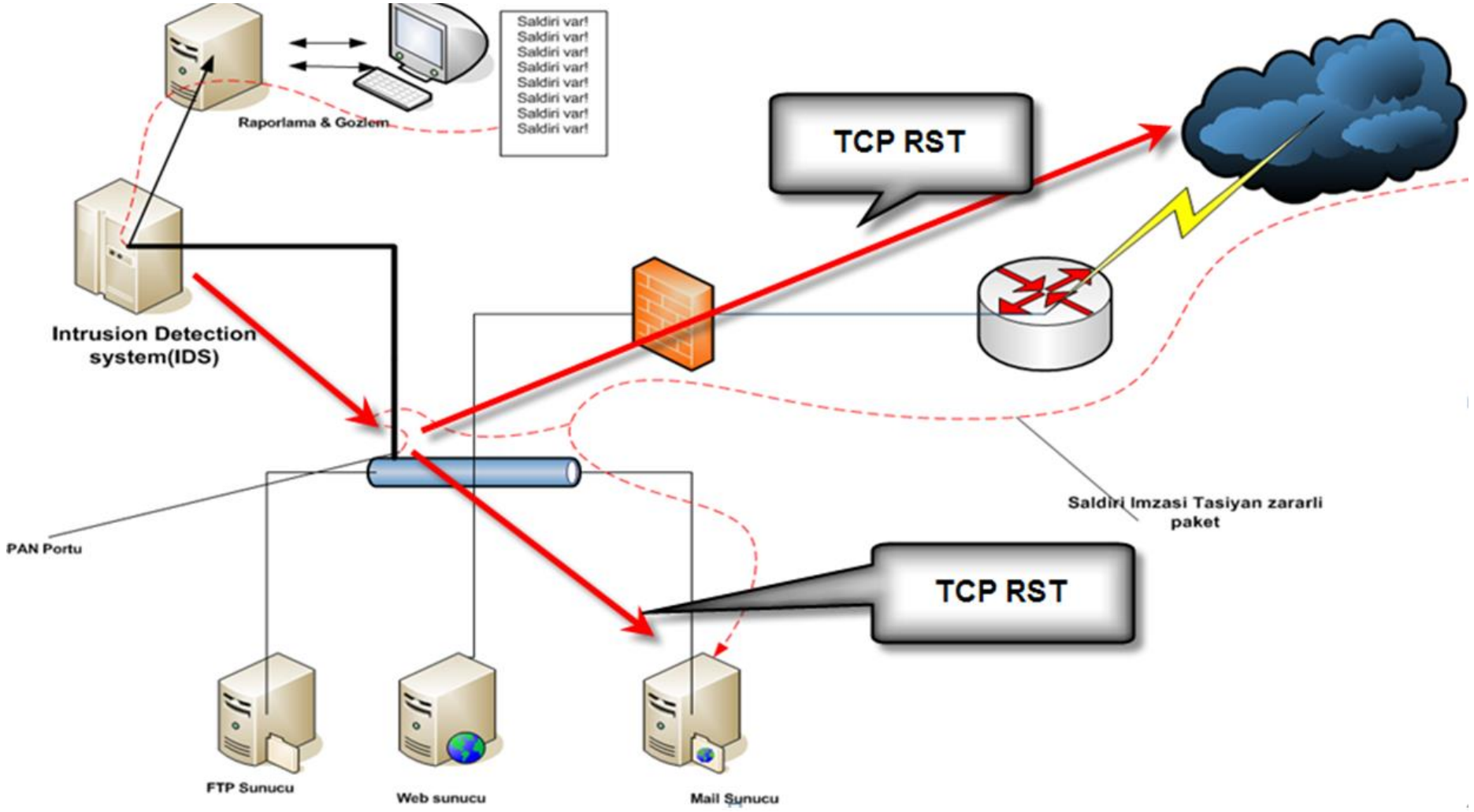
- Arabirim IP adresine sahipse:
  - RAW socketler kullanılır(ön tanımlı durum)
  - Bu modda IP adresi yoksa RST paketleri hedefe ulaşmaz.
- Arabirim IP adresine sahip değilse:
  - Bridge arabirimin MAC adresi kullanılarak RST gönderme işlemi yapılabilir.
  - Bu ayar için snort.conf'ta aşağıdaki değişiklik yapılmalıdır.

```
config layer2resets: 00:06:76:DD:5F:E3
```

Ek Çalışma Modu:Aktif Yanıt Sistemi

- IDS ile IPS arasında geçiş noktası
- IDS olarak çalışan sistemin saldırı yakaladığında saldıran IP adresini engellemesi ya da saldırı paketlerini geçersiz kılması
- Saldırı paketlerine RST/ICMP Unreachable döner ya da Firewall/Router'a komut gönderilir.
- Snort için ActiveResponse uygulamaları
  - FlexResp
  - SnortSam

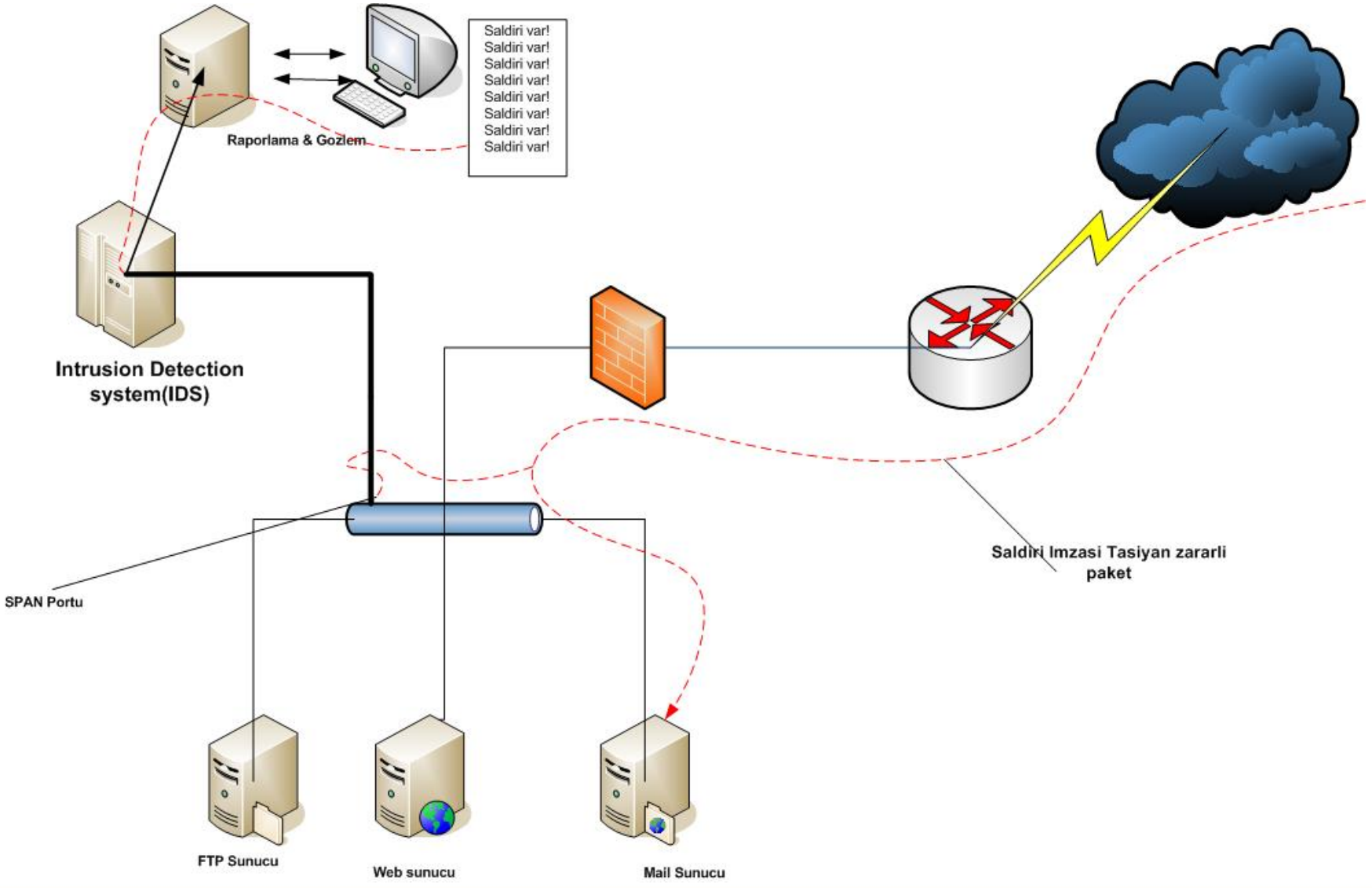
Aktif Yanıt Sistemi



Ek Çalışma Modu: ADS Mod

- ADS=Anomally detection system
- ADS çalışma mantığı: ağ ortamının normal kabul edilecek değerlerini belirleme(sistemin kendisi de öğrenebilmeli)
  - Belirtilen sapma değerini aşan durumlarda anormallik bayrağını kaldırıp uyarı verme
- Snort imzaları kullanılarak ADS mantığı uygulanabilir.
  - Threshold özelliği
- ADS amaçlı olarak Ourmon yazılımı da kullanılabilir.

ADS Mod Yerleşimi



ADS Mod Özellikleri

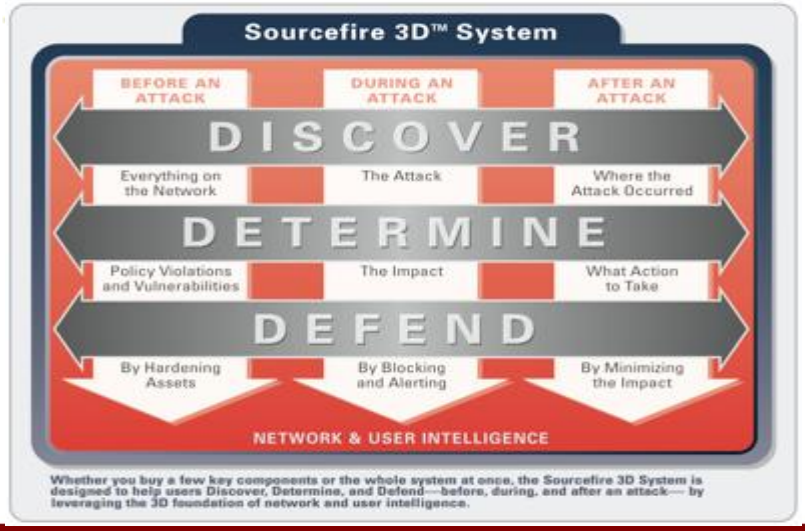
- Hangi anormallikleri keşfedebilir?
- Anormallik tespit sistemlerinin en önemli özelliği normal-anormal durumların belirlenmesidir.
- Snort ADS olarak kullanarak
  - Ağınızdaki botnete üye zombi sistemler
  - Ağınızdan dışarı çıkmaya çalışan saldırı trafikleri
  - Ağınızda dolaşan wormlar
  - Ağınızda dolaşan virüs bulaşmış sistemler
  - Ağınızdan anormal trafik üreten sistemler

  rahatlıkla belirlenebilir!

ADS Mod Nasl Kurulur?

- Gereksiz tüm snort bileşenleri kaldırılır.
- Gereksiz tüm snort kuralları -incelenerek- kaldırılır.
- Span ya da TAP sistemleri kullanılarak tüm trafiğin Snort'a aktarılması(pasif olarak) sağlanır.

Piyasadaki en iyi ADS Sourcefire 3D'dir. Sourcefire, taban olarak Snort kullanmaktadır.



DLP Olarak snort

- Ağ tabanlı veri sızma koruması
  - Ağ üzerindeki trafikte belirlenmiş çeşitli kurallara göre arama yapıp şirkete ait verilerin dışarı çıkmasını engelleme, kaydetme
- Ngrep, snort ağ üzerinden akan "şifresiz" trafiğe ait tüm detayları izleyebilir.
- İstenirse Snort kuralları yazılarak ağ üzerinden geçen belirli özelliklerdeki paketler engellenebilir, kaydedilebilir!

DLP Olarak Snort

- http://cvs.snort.org/viewcvs.cgi/*checkout*/snort/doc/README.sensitive_data?rev=1.1
- http://www.sans.org/security-resources/idfaq/snort-detect-credit-card-numbers.php

```
alert tcp any any <> any any (pcre:"/4\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; \
    msg:"VISA card number detected in clear
text";content:"visa";nocase;sid:9000000;rev:1;)
```

```
alert tcp $HOME_NET $HIGH_PORTS -> $EXTERNAL_NET $SMTP_PORTS \ (msg:"Credit
Card numbers sent over email"; gid:138; sid:1000; rev:1; \ sd_pattern:4,credit_card;
metadata:service smtp;)
```

IDS/IPS Kural/İmzaları

IDS'lerde Kural/İmza Mantığı

- Kural mı imza mı?
  - İmza(signature)= trafik içerisinde "imza(xyz gibi)" arama
  - Kural(Rule)=İmza ve başka parçaları kontrol etme
  - Snort imza tabanlı değil, kural tabanlı bir IPS'dir!
- IDSler iki temel çalışma yöntemi
  - İmza tabanlı
  - Anormallik tabanlı
- İmzalar Vulnerability tabanlı olabilir
- İmzalar Exploit tabanlı olabilir

Kuralları Anlama ve Yorumlama

- Snort yapılandırmasının en önemli bileşenlerinden.
- Saldırı tespit sistemine ne yapacağını söyleyen bileşenlerden
  - Diğer bileşen Preprocessor(önişlemci)

Kural Çeşitleri

- Sourcefire kuralları
  - Ticari kurallar
  - Ücretsiz kurallar(30 gün gecikmeli?)
- SO kurallar
- BE kuralları
- Kendi geliştireceğiniz kurallar

Kural Sınıflandırmaları

- Tüm kurallar tek bir dosyadan alınmaz
- Saldırı kuralları çeşitli kategorilere bölünmüştür.

Makefile.am	info.rules	smtp.rules
VRT-License.txt	local.rules	snmp.rules
attack-responses.rules	misc.rules	specific-threats.rules
backdoor.rules	multimedia.rules	spyware-put.rules
bad-traffic.rules	mysql.rules	sql.rules
cgi-bin.list	netbios.rules	telnet.rules
chat.rules	nntp.rules	tftp.rules
content-replace.rules	open-test.conf	virus.rules
ddos.rules	oracle.rules	voip.rules
deleted.rules	other-ids.rules	web-attacks.rules
dns.rules	p2p.rules	web-cgi.rules
dos.rules	policy.rules	web-client.rules
experimental.rules	pop2.rules	web-coldfusion.rules
exploit.rules	pop3.rules	web-frontpage.rules
finger.rules	porn.rules	web-iis.rules
ftp.rules	rpc.rules	web-misc.rules
icmp-info.rules	rservices.rules	web-php.rules
icmp.rules	scan.rules	x11.rules
imap.rules	shellcode.rules	

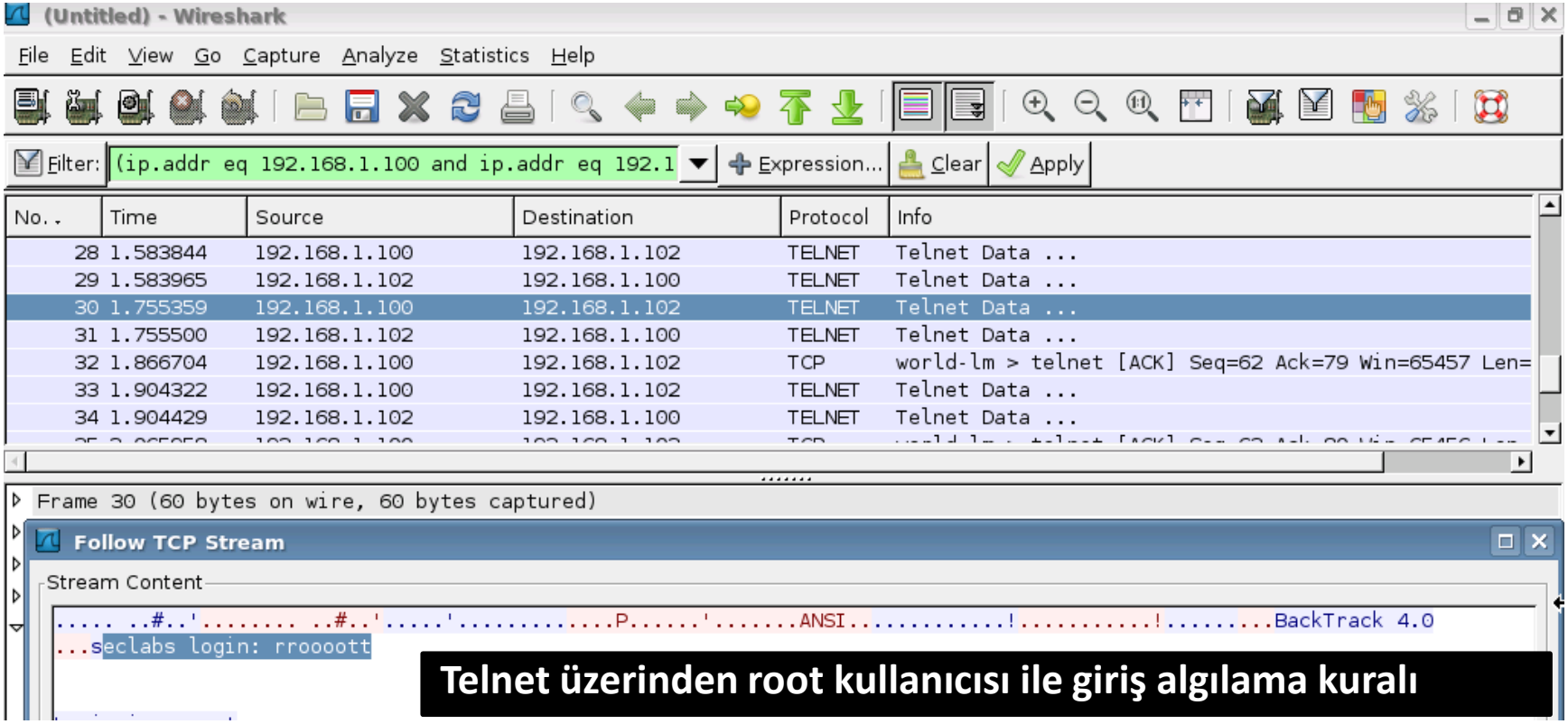
Kural Kategori İşlevleri

Kural Kategorisi	İşlevi
backdoor.rules	*çeşitli trojanlar ve rootkitler tarafında oluşturulan trafiği saptamak için yazılmıştır.*
ddos.rules	*Bilinnen DDOS sa ldırılarını saptamak için kullanılır.*
Oracle.rules	*oracle veritabanı sunucusuna yapılabilecek saldırıları tespit eder.*
scan.rules	*çeşitli ağ ve servis tarama araçlarının yaptığı taramaları tespti eder*
web-iis.rules	*Microsoft IIS'e yapılacak saldırılarıo tespit eder, eğer ağınızda IIS çalışıyorsa bu kural ailesinini aktif edilmesine gerek yoktur.*
p2p.rules	*P2P trafiği tespit etmek için kullanılır*

IDS Kurallarını Anlamak

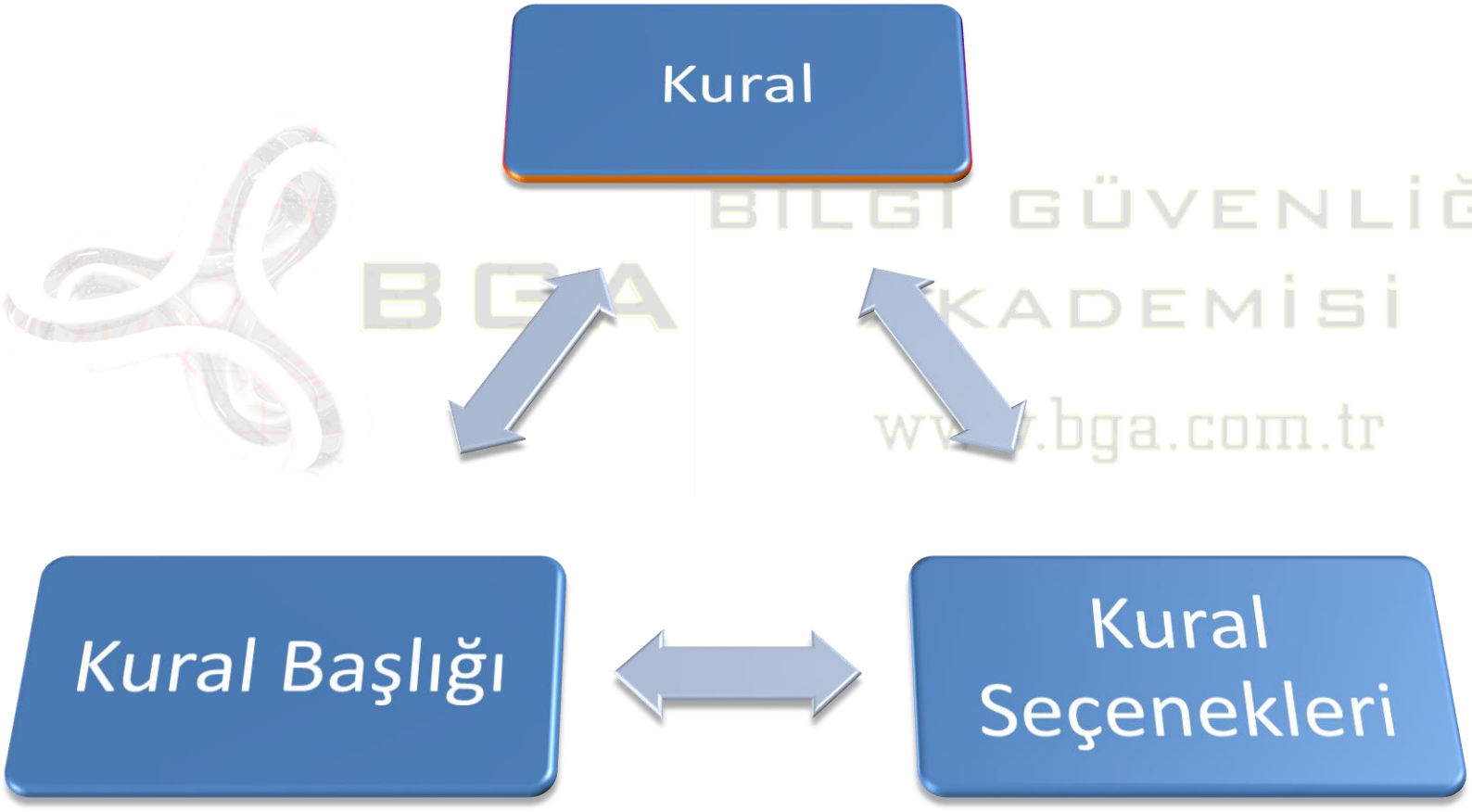
- Oldukça Esnek kural yazma imkanı
- Hazır kuralları kullanma
  - BleedingEdge
  - SourceFire Kuralları
  - Kuralları Güncelleme -OinkMaster
- Kural = Kural Başlığı + Kural Seçenekleri

Basit IDS Kuralı




```
alert tcp $TELNET_SERVERS 23 -> $EXTERNAL_NET any (msg:"TELNET root
    login"; content:"login\: root";
flow:from_server,established; classtype:suspicious-login; sid:719; rev:5;)
```

Snort Kuralları



Kural Başlık/Seçenekleri

- Her kuralda bir adet kural başlığı ve kural seçeneği bulunur.
- Snort Kurallarının gücü kural seçeneklerindedir.
- Kural başlıkları Firewall benzeri mantıkla çalışır.

Kural Başlığı	Kural Seçenekleri
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: SF; msg: “SYN-FIN Scan”;)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: S12; msg: “Queso Scan”;)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: F; msg: “FIN Scan”;)

Kural Başlığı:Aksiyon

- Snort kural başlığının en önemli alanlarından biridir ve imzaya uyan paket için ne yapılacağını belirtir.

```
alert tcp 192.168.0.0/24 any -> 10.10.10.180
```

Aksiyon	İşlevi
Alert	Uyan paketler için uyarı vermek ve loglamak için
Log	Uyarı vermden sadece loglamak için
Pass	Paketi önemseme
Activate	Uyarı verip dinamik bir kuralı tetiklemek için
Dynamic	Activate aracılığı ile gelen emirleri bekleyerek işleme almak için
Drop	Iptables'ın paketi bloklaması ve loglaması için
Sdrop	Iptables'in paketi bloklaması için.(Loglama yok)
Reject	Iptables'in saldırgana TCP RST ya d aIcmp port unreachabel mesajı göndererek loglaması için.

Kural Başlığı: Protokol Alanı

alert tcp 192.168.0.0/24 any -> 10.10.10.180

Hangi Protokolü incelediğini belirtir
Aşağıdaki değerleri alabilir
- **TCP**
- **UDP**
- **ICMP**
- **IP**

Kural Başlığı: IP Adres Alanı

```
alert tcp 192.168.0.0/24 any -> 10.10.10.180
```

Kaynak IP: Trafiğin nerden geldiğini belirtir.

- CIDR olabilir.
- Tek bir IP Adresi olabilir.
- Netmask olabilir.
- Önüne ! Koyarak hariç tutulabilir.
- Any özel kelimesiyle tüm IP adresleri kastedilebilir.
- $HOME_NET gibi değişken tanımları kullanılabilir.

Kural Başlığı: IP Adres Alanı

```
alert tcp 192.168.0.0/24 any -> 10.10.10.180
```

HedefIP: Trafiğin nerye gittiğini belirtir
- CIDR olabilir
- Tek bir IP Adresi olabilir
- Netmask olabilir
- Önüne ! Koyarak hariç tutulabilir
- Any özel kelimesiyle tüm IP adresleri kastedilebilir
- $HOME_NET gibi değişken tanımları kullanılabilir

Kural Başlığı: Port Alanı

alert tcp 192.168.0.0/24 any -> 10.10.10.1 80

Port : Trafiğin hangi porttan gelip hangi porta gittiğini belirtir

- 80, 110, 443 gibi bir değer alabilir
- Önüne ! Koyarak hariç tutulabilir (!80)
- Any özel kelimesiyle tüm port numaraları kapsanabilir
- 22:900 gibi aralık verilebilir
- $ORACLE_PORTS gibi değişken tanımları kullanılabilir
- Büyüktür, küçüktür ifadeleri kullanılabilir (:1024, 2200:) gibi

Kural Başlığı:Yön

alert tcp 192.168.0.0/24 any -> 10.10.10.1 80

Trafiğin sol taraftan sağ tarafa doğru aktığını belirtir
->
<>
İfadeleri kullanılabilir

Kural Seçenekleri

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS \
(msg:"WEB-MISC rcmd attempt"; flow:to_server,established; uricontent:"rcmd.exe"; nocase; \
metadata:service http; classtype:web-application-activity; sid:1065; rev:8;)
```

Kural Başlığı

Kural Seçenekleri

- Detection Engine'nin kalbi sayılır
- () arasına yazılır ve birbirinden ";" ile ayrılır
- () arasına almak zorunludur
- Her seçenek ; ile biter, son seçenek dahil!
- Seçenek ve alacağı değer : ile ayrılır
- Meta-data, payload, non-payload, post-detection alanlarına ayrılır.

Metadata

- Kural hakkında çeşitli bilgiler vermek için
  - Raportlama ve analiz aşamasında kullanılır.
- Msg Kural tetiklendiğinde verilecek mesaj
  - (msg:"WEB-MISC rcmd attempt"; ...
- Sid Snort kural ID
  - sid:1065;
  - Kural numaraları(0-100 arası kullanılmaz)
- Rev Kuralın kaç revizyon geçirdiği
  - id:1065; rev:8;

Metadata-II

- Reference: Tetiklenen kuralla ilgili detay bilgileri içeren referanslar
  - reference:url,www.securiteam.com/exploits/3D5Q4RFPPK.html;
- Classification: Kuralı sınıflandırma amaçlı
  - classtype: trojan-activity;
- Priority: Kurala önem tanımlama
  - Düşük değer daha yüksek öneme sahiptir.

Kural Yazımı-Non Payload Detection

- Protokollerin başlıkları ile ilgilenir
  - TTL Alanı kontrolü ttl:<3;
- IP Tos Alanı kontrolü tos:8; (Minimize Delay)
- Ipopts Alanı Kontrolu
  - Record route, IP security option , Loose source routing , any IP options are set
- Fragbits
  - IP parçalanma alanını kontrol eder
- Flags: TCP Bayraklarını kontrol eder
  - (msg:"SCAN nmap XMAS"; stateless; flags:FPU,12;

http://www.procyonlabs.com/snort_manual/node1.html

Kural Seçenekleri:IP

- Fragoffset
- Ttl
- İd
- Tos
- ipopts
- Fragbits
- Dsize
- İp_proto
- Sameip

Kural Seçenekleri:IP->TTL

- IP başlığındaki TTL alanını kontrol etmek için kullanılır
  - ttl:[[<number>-]><=]<number>;
- Örnek kullanım
  - ttl:<2;
  - ttl:1-3;
- Traceroute yakalama

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP traceroute"; itype:8; ttl:<2; reference:arachnids,118; classtype:attempted-recon; sid:385; rev:4;)

Kural Seçenekleri:IP->sameip

- Kaynek ve hedef ip adreslerinin aynı olup olmadığını kontrol eder
  - Land attack
- alert ip any any -> any any (sameip;)

Kural Seçenekleri:IP->ipopts

- Gelen-giden paketlerde herhangi bir IP seçeneğinin olup olmadığını kontrol eder

```
alert ip $EXTERNAL_NET any -> $HOME_NET any
(msg:"MISC source route ssrr"; ipopts:ssrr ;
reference:cve,1999-0510; classtype:bad-unknown;
sid:502; rev:4;)
```

rr
- Record Route

eol
- End of list

nop
- No Op

ts
- Time Stamp

sec
- IP Security

esec
- IP Extended Security

lsrr
- Loose Source Routing

ssrr
- Strict Source Routing

satid
- Stream identifier

any
- any IP options are set

Kural Seçenekleri:TCP

- TCP başlık bilgilerini kontrol etmek için kullanılır
  - Flags
  - Seq
  - Ack
  - Flow
  - stateless

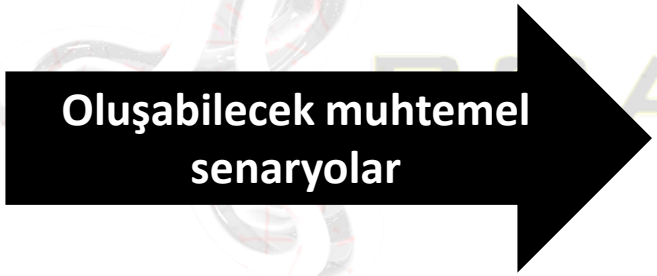
Kural Seçenekleri:TCP->Flags

- Gelen pakette hangi bayrakların set edildiğini bulmaya yarar
  - flags:[!|*|+]<FSRPAU120>[,<FSRPAU120>];


```
alert tcp any any -> any any (flags:SF,12;)
```

Kural Seçenekleri:TCP->Flow

- TCP oturum durumunu kontrol eder



Option	Description
to_client	Trigger on server responses from A to B
to_server	Trigger on client requests from A to B
from_client	Trigger on client requests from A to B
from_server	Trigger on server responses from A to B
established	Trigger only on established TCP connections
stateless	Trigger regardless of the state of the stream processor (useful for packets that are designed to cause machines to crash)
no_stream	Do not trigger on rebuilt stream packets (useful for dsize and stream5)
only_stream	Only trigger on rebuilt stream packets

alert tcp !$HOME_NET any -> $HOME_NET 21 (msg:"cd incoming detected"; \ flow:from_client; content:"CWD incoming"; nocase;)

Kural Seçenekleri:ICMP

- ICMP başlık bilgilerini inceleyen kural seçeneği
- İtype
- İcode
- İcmp_seq
- İcmp_id

Değerlerini alabilir.

Kural Seçenekleri:Dsize

- Paket “payload” kısmının boyutunu ölçmek için kullanılır.
  - dsize: [<>]<number>[<><number>];

alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433:1500 (msg:"SQL Microsoft SQL Server 2000 Server hello buffer overflow attempt"; flow:to_server,established; **dsize:>511;** content:"|12 01|"; depth:2; content:!"|00|"; within:512; distance:35; reference:bugtraq,5411; reference:cve,2002-1123; reference:url,www.microsoft.com/technet/security/Bulletin/MS02-056.mspx; classtype:attempted-admin; sid:11264; rev:5;)

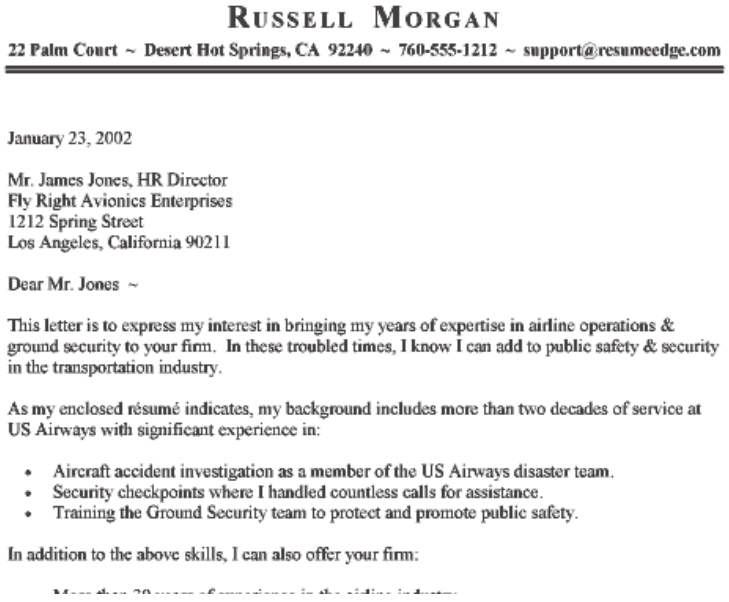
Tüm Non-Payload Seçenekleri

Keyword	Description
fragoffset	The fragoffset keyword allows one to compare the IP fragment offset field against a decimal value.
ttl	The ttl keyword is used to check the IP time-to-live value.
tos	The tos keyword is used to check the IP TOS field for a specific value.
id	The id keyword is used to check the IP ID field for a specific value.
ipopts	The ipopts keyword is used to check if a specific IP option is present.
fragbits	The fragbits keyword is used to check if fragmentation and reserved bits are set in the IP header.
dsize	The dsize keyword is used to test the packet payload size.
flags	The flags keyword is used to check if specific TCP flag bits are present.
flow	The flow keyword allows rules to only apply to certain directions of the traffic flow.
flowbits	The flowbits keyword allows rules to track states during a transport protocol session.

seq	The seq keyword is used to check for a specific TCP sequence number.
ack	The ack keyword is used to check for a specific TCP acknowledge number.
window	The window keyword is used to check for a specific TCP window size.
itype	The itype keyword is used to check for a specific ICMP type value.
icode	The icode keyword is used to check for a specific ICMP code value.
icmp_id	The icmp_id keyword is used to check for a specific ICMP ID value.
icmp_seq	The icmp_seq keyword is used to check for a specific ICMP sequence value.
rpc	The rpc keyword is used to check for a RPC application, version, and procedure numbers in SUNRPC CALL requests.
ip_proto	The ip_proto keyword allows checks against the IP protocol header.
sameip	The sameip keyword allows rules to check if the source ip is the same as the destination IP.

Payload

- Paketin içerisini incelenen kural seçenek kısmı



RUSSELL MORGAN
22 Palm Court ~ Desert Hot Springs, CA 92240 ~ 760-555-1212 ~ support@resumeedge.com

January 23, 2002

Mr. James Jones, HR Director
Fly Right Avionics Enterprises
1212 Spring Street
Los Angeles, California 90211

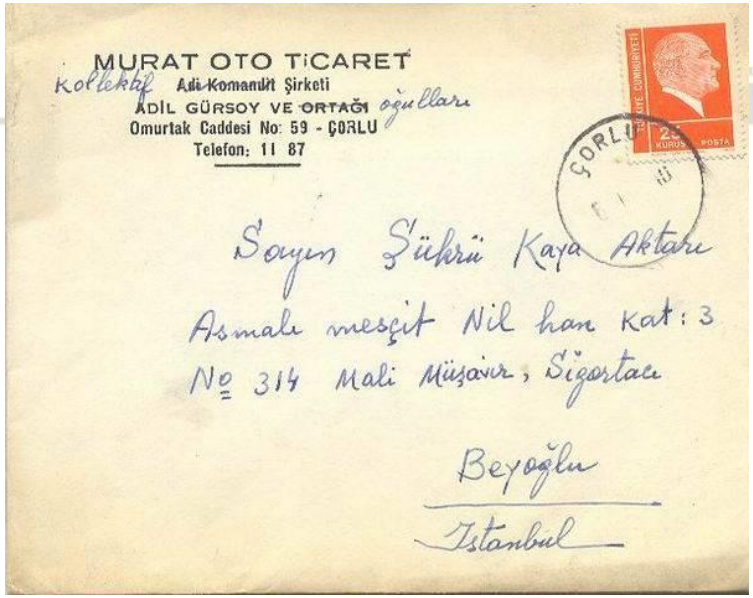
Dear Mr. Jones ~

This letter is to express my interest in bringing my years of expertise in airline operations & ground security to your firm. In these troubled times, I know I can add to public safety & security in the transportation industry.

As my enclosed résumé indicates, my background includes more than two decades of service at US Airways with significant experience in:

- Aircraft accident investigation as a member of the US Airways disaster team.
- Security checkpoints where I handled countless calls for assistance.
- Training the Ground Security team to protect and promote public safety.

In addition to the above skills, I can also offer your firm:



MURAT OTO TİCARET
Kollektif Adi Komandit Şirketi
ADİL GÜRSOY VE ORTAĞI oğulları
Omurtak Caddesi No: 59 - ÇORLU
Telefon: 11 87

ÇORLU

Sayın Şükrü Kaya Aktaru
Asmalı mescit Nil han Kat: 3
No 314 Mali Müşavir, Sigortacı
Beyoğlu
İstanbul

PAYLOAD

HEADER

Kural Seçenekleri:Content

- Paket veri alanında spesifik içerik tarama için kullanılır.
  - content: [!] "<content string>";
- Binary(ikili) içerik için | 00 0F| kullanılır (hex)
- Bir kural da hem text hem hex değerler bulunabilir.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 (msg:"IMAP login brute force
attempt"; flow:to_server,established; content:"LOGIN"; nocase;
```

Kural Seçenekleri:Nocase

- Content için arama yapılırken büyük küçük harf ayrımı yapılmayacağını belirtir.


```
alert tcp any any -> any 21 (msg:"FTP ROOT";
content:"USER root"; nocase;)
```

Kural Seçenekleri:Offset

- “Content” için arama işleminin payload’un neresinden başlanacağını belirtir.
  - 300K lık bir paket içerisinde 3K’lık bir arama için tüm paketi dolaşmak gereksiz ve perfomans yorucudur
- Offset bir önceki content: tanımını etkiler

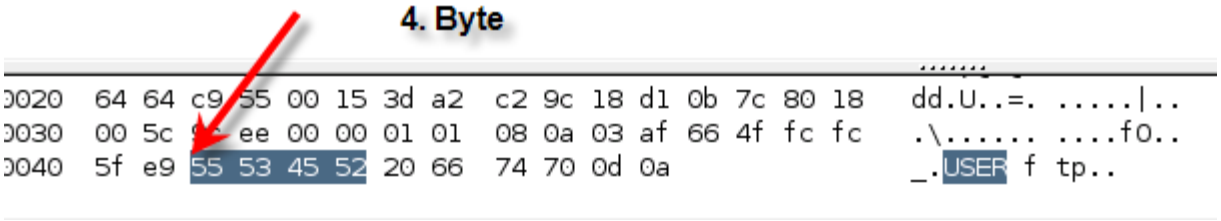

```
alert tcp any any -> any 80 (content: "cgi-bin/phf"; offset:4; depth:20;)
```

Kural Seçenekleri:Depth

- Snort'un kaç byte'lık dilime bakacağını belirtir
- Bir önceki "content:" seçeneğini etkiler

```
alert tcp any any -> any 80 (content: "cgi-bin/phf"; offset:4;
depth:20;)
```

- 4. Byte'dan başla 20 Byte incele...



Kural Seçenekleri:Distance

- Bir önceki “content:” tanımlamasından ne kadar byte ileri gidileceğini belirtir.
- Content:”A”; content:”C”; distance:1
  - A ile C arasında bir boşluk var
- ABC ile başlayıp -arada bir karekter herhangi birşey gelebilir- DEF ile biten içerik araması

```
alert tcp any any -> any any (content:"ABC"; content:
"DEF"; distance:1;)
```

Kural Seçenekleri:Within

- Bir önceki “content:” den sonra ne kadarlık bir alan içerisinde ikinci “content” in araştırılacağını belirler.
- ABC’den sonra 10 byte içerisinde EFG ara

```
alert tcp any any -> any any (content:"ABC"; content: "EFG"; within:10;)
```

Kural Seçenekleri:UriContent

- HTTPInspect önişlemcisi tarafından normalleştirilmiş HTTP trafiği içerisindeki URL kısmını inceler.
- uricontent:[!]<content string>;

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"SPYWARE-PUT Adware gophoria toolbar runtime detection"; flow:to_server,established; **uricontent:"/application/app_counter/?gopver=";** nocase; reference:url,www.360zd.com/spyware/518.html; classtype:misc-activity; sid:12791; rev:1;)

Görünmez İçerik Filtreleme Sistemi

- URIContent özelliği kullanılarak L2 modda (üzerinde IP adresi olmayan) içerik filtreleme yapılabilir.
  - Uricontent:”http://www.google.com”
- Youtube yasağına çözüm!
  - Uricontent:”http://www.youtube.com/videoid?901”

Kural Seçenekleri:http_header

- HTTP istek ve cevapları için kullanılır

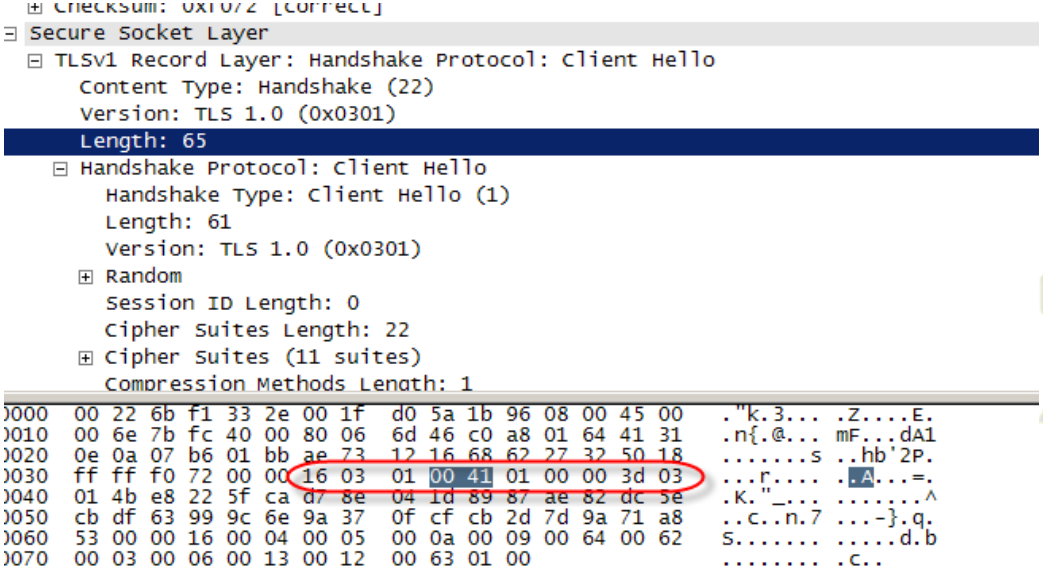

```
alert http $HOME_NET any -> $EXTERNAL_NET any (\
msg:"ET P2P ABC Torrent User-Agent (ABC/ABC-3.1.0)"; \
header.useragent:"ABC/ABC"; \
sid:2003475;)
```

Kural Seçenekleri:Pcre

- PCRE = Perl compatible regular expressions
- Regex yazım kuralları bilinmelidir.
  - http://www.pcre.org
- Performans canavarıdır!
  - Çok gerekmedikçe kullanılmamalıdır.


```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-PHP gallery
arbitrary command execution attempt"; flow:to_server,established; uricontent:"/setup/";
content:"GALLERY_BASEDIR="; pcre:"/GALLERY_BASEDIR=(http|https|ftp)/i";
reference:nessus,11876; reference:bugtraq,8814; classtype:web-application-attack; sid:2306;
rev:2;)
```

Ultrasurf Engelleme Kuralı



1603010041010000 3d0301 hex ifadesinde normal TLS bağlantılarından farklı tek şey Length değerleri.

16: Content Type: Handshake

03 01: Version TLS1.0

00 41: Length 65

01: Handshake Type: Client Hello

00 00 3d: Length 61

03 01:Version TLS1.0

alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"Ultrasurf Kullanimi!"; flow:to_server,established; content:"|1603010041010000 3d0301|"; classtype:policy-violation; sid:1000099;)

Hangi Kural Ne İşe Yarar?

Sid	Summary	Impact	Detailed Information	Affected Systems	Attack Scenarios	Ease of Attack	False Positive	False Negative	Corrective Action	Contributors	Additional References
1:1520	This event is generated when an attempt is made to access server-info. Using the Apache webserver, this url is generally handled by the mod_info module, which will happily disclose valuable information about your webserver which may aid in their attack.	Information disclosure.	The mod_info module "provides a comprehensive overview of the server configuration including all installed modules and directives in the configuration files" for the Apache webserver. Successfully accessing the url that is handle by mod_info may give an attacker valuable information about the server. If mod_info is in use and the attacking host is allowed to access it, every possible configuration option that the Apache server is using can be viewed. This includes ACLs, modules, file and directory names, and other valuable information that will help an attacker determine ways of attacking the server.	Apache webservers with mod_info enabled.	As part of an attack against an Apache webserver, an attacker may try to access "/server-info" which is typically handled by the mod_info module. If sucessful, this will give valuable information about the webserver for use in further attacks.	Simple. No exploit software is required.	Few, but certainly possible. Since this rule only checks for the existance of "/server-info" in the url, any url containing that string will trigger this rule. A few common false positives may include urls like: http://victim /server-info/contact.html http://victim /really /long/directory /server-info.html	None Known	Determine if server-info exists on the victim in question, and if the attacker is allowed to access it. If mod_info is necessary on this server, consider restricting access to it via Apache directives, i.e.: SetHandler server-info Order deny,allow Deny from all Allow from .yourdomain.net	Snort documentation contributed by Jon Hart Sourcefire Vulnerability Research Team Brian Caswell Nigel Houghton	

Örnek Kural-#1

```
alert tcp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD-TRAFFIC tcp port 0 traffic";
flow:stateless; classtype:misc-activity; sid:524; rev:9;)
```

Örnek Kural-#2

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS zone transfer TCP";
flow:to_server,established; content:"|00 00 FC|"; offset:15; metadata:policy
security-ips drop, service dns; reference:arachnids,212; reference:cve,1999-0532;
reference:nessus,10595; classtype:attempted-recon; sid:255; rev:16;)
```

Örnek Kural-#3

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP traceroute";
itype:8; ttl:1; reference:arachnids,118; classtype:attempted-recon; sid:385; rev:4;)
```

Örnek Kural-#4

- Port tarama(nmap -sS)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -
sS window 2048"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:20
48; classtype:attempted-recon;
reference:url,doc.emergingthreats.net/2000537;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.c
gi/sigs/SCAN/SCAN_NMAP; sid:2000537; rev:7;)
```

```
[**] [1:2009584:1] ET SCAN NMAP -sS window 4096 [**]
[Classification: Attempted Information Leak] [Priority: 2]
04/29-23:24:06.440226 88.240.10.125:50548 -> 212.98.228.246:80
TCP TTL:52 TOS:0x0 ID:38946 IpLen:20 DgmLen:60
******S* Seq: 0x22700D04  Ack: 0x0  Win: 0x1000  TcpLen: 40
TCP Options (6) => MSS: 1452 NOP WS: 0 NOP NOP TS: 17745 0
[Xref => http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/S
```

Örnek Kural-#5

- /etc/passwd

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC
/etc/passwd"; flow:to_server,established; content:"/etc/passwd"; nocase;
metadata:service http; classtype:attempted-recon; sid:1122; rev:6;)
```

Örnek Kural-#6

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"P2P Skype client login"; flow:to_client,established; flowbits:isset,skype.login; dsize:5; content:"|17 03 01 00|"; depth:4; metadata:policy security-ips drop; classtype:policy-violation; sid:5999; rev:4;)

Örnek Kural-#7

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"P2P Skype client login"; flow:to_client,established; flowbits:isset,skype.login; dsize:5; content:"|17 03 01 00|"; depth:4; metadata:policy security-ips drop; classtype:policy-violation; sid:5999; rev:4;)

DNS DOS Saldırısı

```
alert udp $HOME_NET 53 -> $EXTERNAL_NET any (msg:"DOS DNS root
query response traffic amplification attempt";\
flow:to_client; content:"|00 01|"; depth:2; offset:4; content:"|00 00 02
00 01|"; within:5; distance:6;\
threshold:type threshold, track by_dst, count 5, seconds 30;
metadata:service dns;\
reference:url,isc.sans.org/diary.html?storyid=5713; classtype:misc-
activity; sid:15260; rev:1;)
```

BGA İletişim

www.bga.com.tr

blog.bga.com.tr

twitter.com/bgasecurity

facebook.com/BGAkademisi

bilgi@bga.com.tr

egitim@bga.com.tr