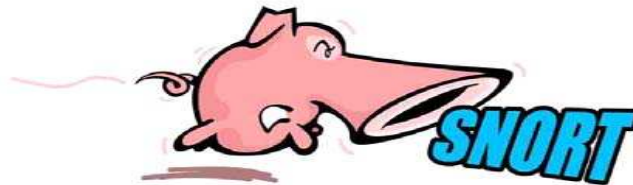


# Açık Kaynak kodlu Yazılımlarla Trafik Analizi, Saldırı Tespiti Ve Engelleme

Huzeyfe ÖNAL

[huzeyfe@lifeoverip.net](mailto:huzeyfe@lifeoverip.net)

<http://www.lifeoverip.net>

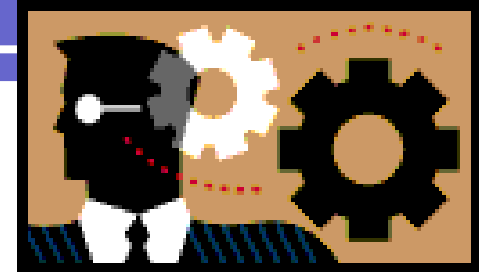


# Sunum Planı



- Açık Kod Trafik Analiz Araçları
- Saldırı Tespit ve Engelleme Sistemleri
- Açık kod Saldırı Tespit sistemi Snort
- Snort'a Giriş
- Snort'un (N)IDS olarak Kullanımı
- Snort'u (N)IPS olarak Kullanmak
- (N)IDS/(N)IPS Atlatma Teknikleri ve Korunma yolları

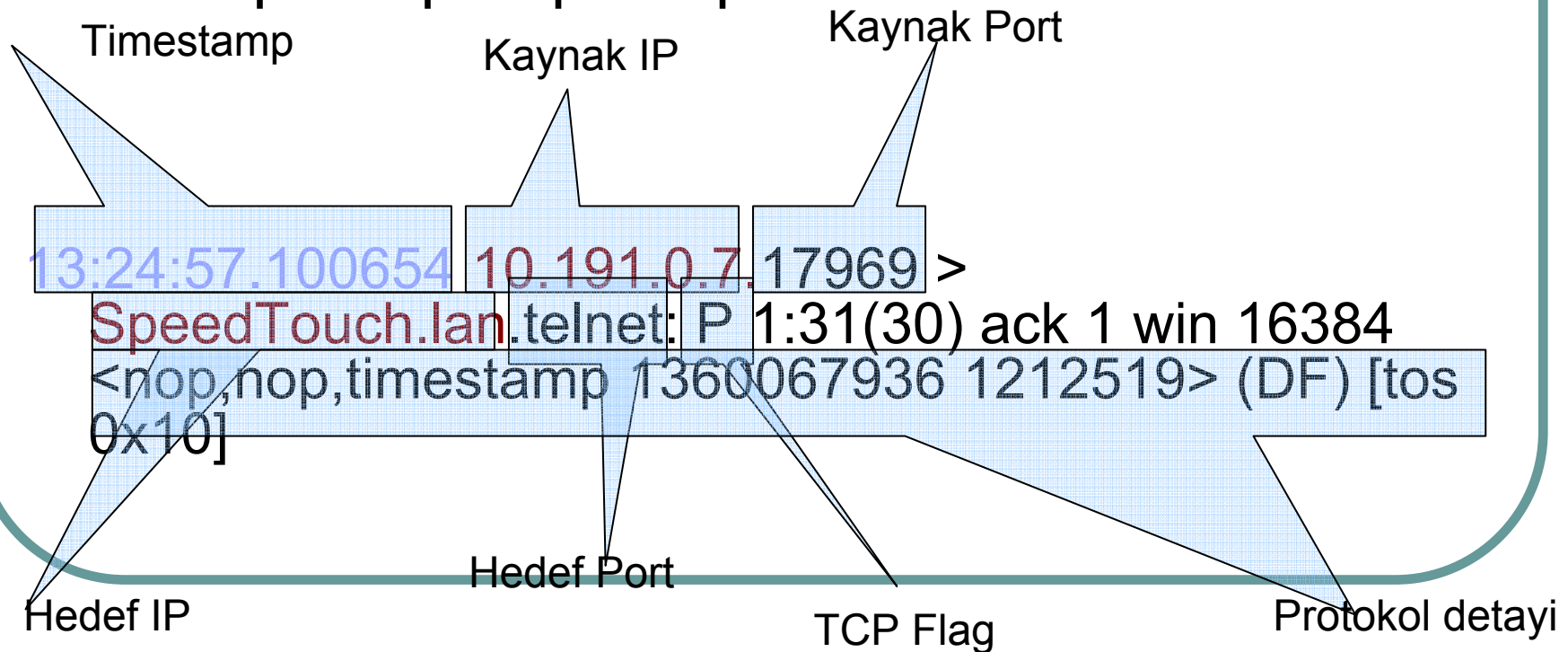
# Trafik analizi



- İletişim == Ağ Trafiki == 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
- Bilişim suçları için adli analiz imkanı

# tcpdump

- En temel unix paket dinleme aracı
- Gelişmiş filtreleme imkanı
  - Tcpdump udp dst port 53



# WireShark/Ethereal

**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: USRobotics\_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)  
Transmission Control Protocol (80), Seq: 1, Ack: 1, Len: 0

**Shell - Konsole**

```
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; charse
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" cellspacing="0" cellpadding="0">
```

**Ethereal: Capture from eth1**

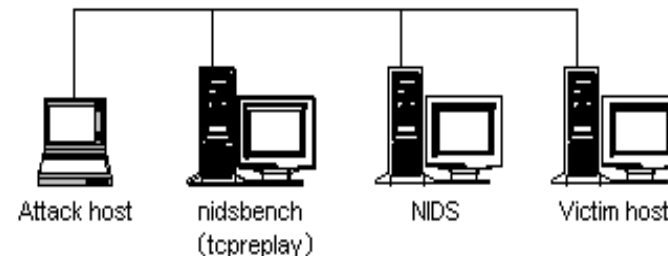
Captured Packets	Total	% of total
Total	31	
SCTP	0	0.0%
TCP	31	100.0%
UDP	0	0.0%
ICMP	0	0.0%
ARP	0	0.0%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	0	0.0%

Running 00:01:40  
Stop

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

# Tcpreplay

- Tcpdump ile kaydedilen(libpcap format) trafiği tekrar oluşturmak için
- Genellikle IDS, Firewall, router, ağ uygulamaları test amaçlı kullanılır
  - Tcpprep:
  - Tcprewrite:
  - Tcpbridge:
  - Flowreplay:
- Tcponera: Gelişmiş Tcpreplay

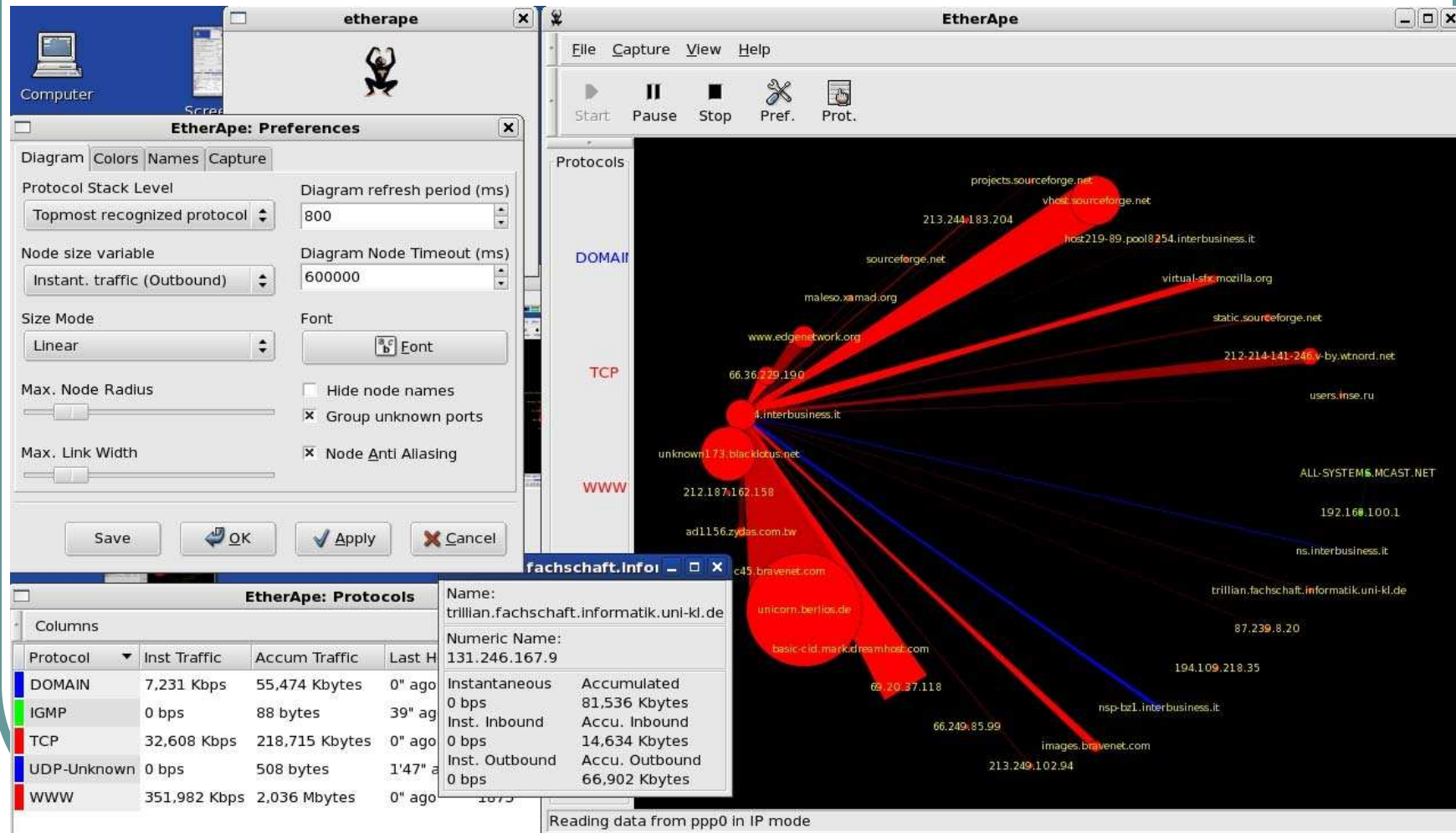


# tcpreplay -i rl0 for\_ab

75 packets successfully sent in 0.002435 seconds(30800.821355 packets per second)

5187 bytes successfully sent(2130184.804928 bytes per second  
16.252020 megabits per second)

# LAN izleme: Etherape



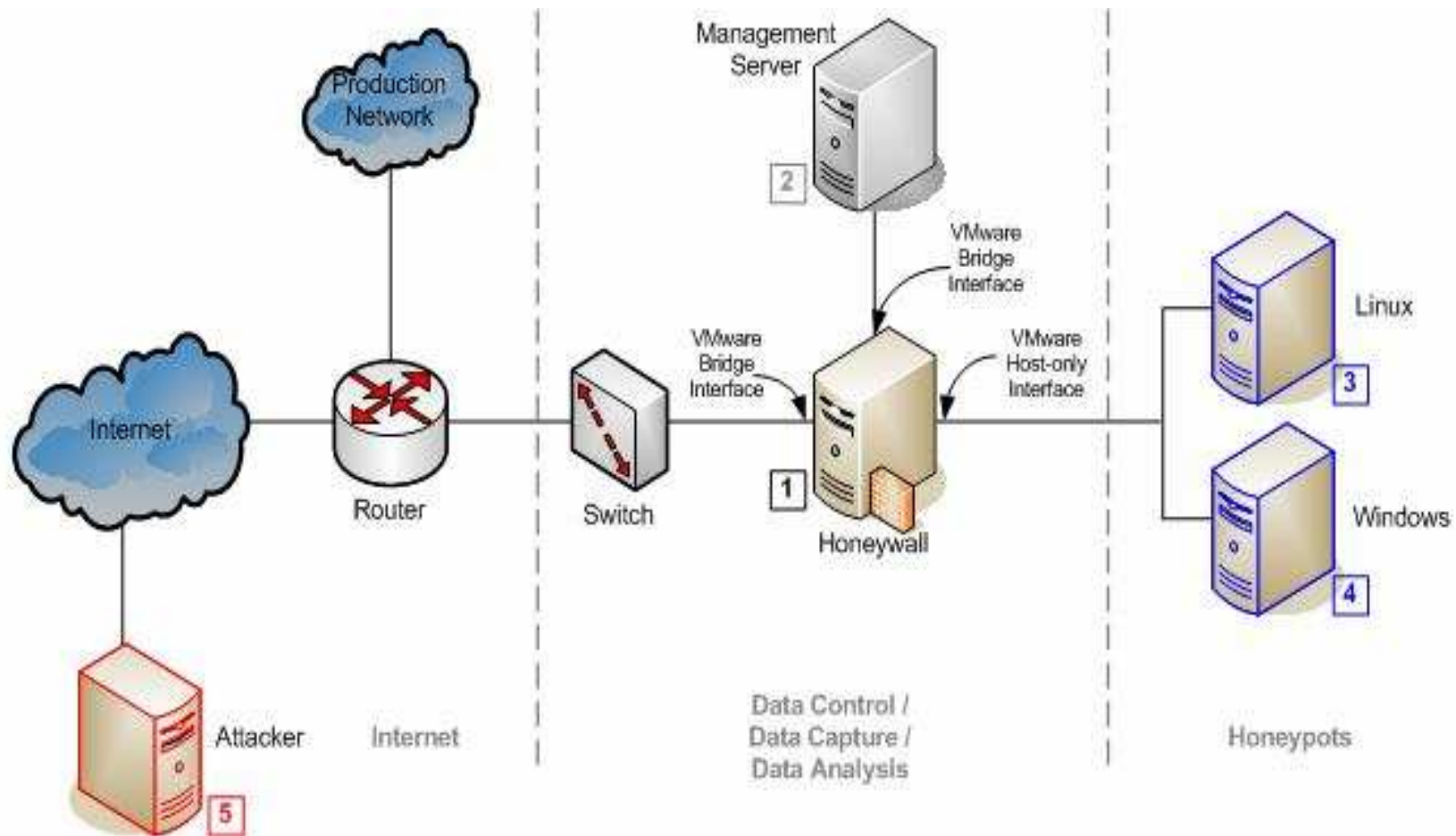


# Tuzak Sistemler

- Yeni(?) bir konsept..
  - Düşmanın teknolojisini bilerek savaşıma
- Yapılan saldırılar incelenerek önlem alma kolaylığı
- Honeynet Projesi
  - Siyah sapkaların kullandığı yöntemlerin , motivasyonların incelenmesi ve sonuçların paylaşımı
  - <http://www.honeynet.org> 2002 –
- Honeypot
  - Düşük seviye etkileşimli - servis simülasyonu
  - Yüksek seviye etkileşimli – işletim sistemi simülasyonu
  - Sanal - Vmware, UML
  - Fiziksel - maliyet
- Honeyd



# Basit bir HoneyPot

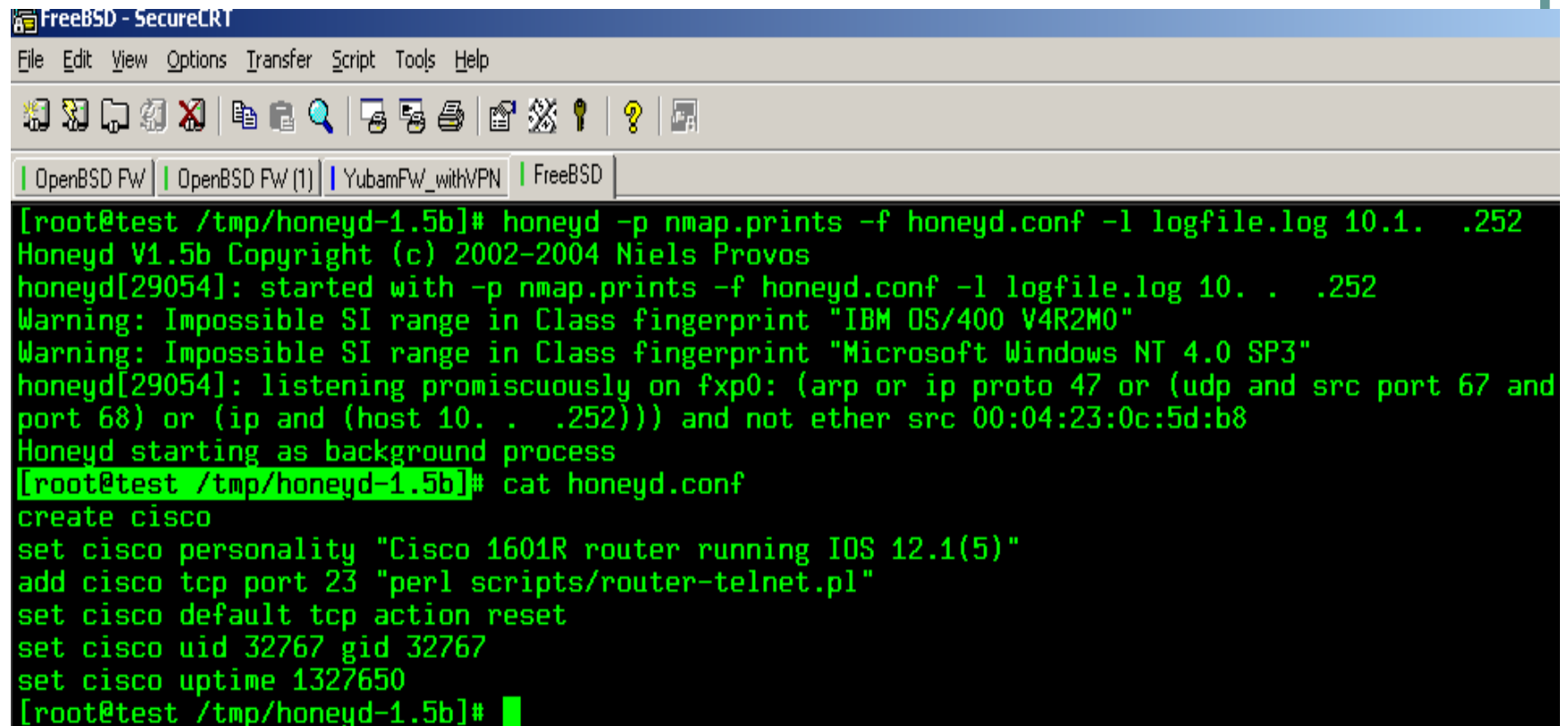


# Honeyd



- Linux/FreeBSD/OpenBSD/Windows'u destek
- Ağdaki boş IP adreslerini kullanabilir
  - Arpd cevap donulmeyen ipler için mac adresi yayımlar
- Eşzamanlı istenilen sayıda işletim sistemi, servis simulasyonu
- İşletim sistemlerini TCP/IP stack seviyesinde simule edebilme(nmap, Xprobe kandırma yeteneği)
- Spam, worm, illegal trafik tespiti için ideal
- Script dilleri ile yeni servis, sistem tanımlama
- Çalıştığı sistemin hacklenme olasılığı !!
- Örnek Kullanım;

# Honeyd



The screenshot shows a terminal window titled "FreeBSD - SecureCRT". The menu bar includes "File", "Edit", "View", "Options", "Transfer", "Script", "Tools", and "Help". The toolbar contains various icons for file operations and terminal control. The tab bar shows four tabs: "OpenBSD Fw", "OpenBSD Fw (1)", "YubamFW\_withVPN", and "FreeBSD", with "FreeBSD" being the active tab. The terminal output shows the execution of the "honeyd" command with specific options, followed by status messages and a warning. Then, the "cat" command is used to display the contents of the "honeyd.conf" file, which configures a Cisco 1601R router.

```
[root@test /tmp/honeyd-1.5b]# honeyd -p nmap.prints -f honeyd.conf -l logfile.log 10.1. .252
Honeyd V1.5b Copyright (c) 2002-2004 Niels Provos
honeyd[29054]: started with -p nmap.prints -f honeyd.conf -l logfile.log 10. . .252
Warning: Impossible SI range in Class fingerprint "IBM OS/400 V4R2M0"
Warning: Impossible SI range in Class fingerprint "Microsoft Windows NT 4.0 SP3"
honeyd[29054]: listening promiscuously on fxp0: (arp or ip proto 47 or (udp and src port 67 and
port 68) or (ip and (host 10. . .252))) and not ether src 00:04:23:0c:5d:b8
Honeyd starting as background process
[root@test /tmp/honeyd-1.5b]# cat honeyd.conf
create cisco
set cisco personality "Cisco 1601R router running IOS 12.1(5)"
add cisco tcp port 23 "perl scripts/router-telnet.pl"
set cisco default tcp action reset
set cisco uid 32767 gid 32767
set cisco uptime 1327650
[root@test /tmp/honeyd-1.5b]#
```

# Network Data carving



- Ham veriden orijinal veri elde etme yöntemi
- Ağ trafiğinizde neler akıyor?
- Örnek;
- **#tcpdump -s0 host www.enderunix.org -w enderunix**
- arkasından wget ile EnderUNIX altından bir gif dosyası indiriyoruz ve chaosreader ile enderunix dosyasına kaydettiğim trafiği okutuyoruz, sonuç?
- **\$perl chaosreader0.94 enderunix**
- Araçlar
  - Chaos Reader, tcpflow, Driftnet..

# Driftnet Kullanımı

The screenshot illustrates the Driftnet tool in use. It consists of three main windows:

- driftnet**: A window showing network traffic analysis. It displays a list of IP addresses and their corresponding data sizes. Below this, it shows a packet capture for Frame 3 (66 bytes on wire, 66 bytes captured). The packet details include Ethernet II, Src: Intel\_d8:df:c9 (00:0c:29:d8:df:c9), and Internet Protocol Src: 192.168.1.2. A 'Shell - Konsole' window is also visible, showing a telnet session to www.enderunix.org and the resulting HTML output.
- Shell - Driftnet**: A terminal window displaying the Driftnet help text and usage instructions. The text includes: "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." It also provides the copyright information (2001-2002 Chris Lightfoot) and the home page (http://www.ex-parrot.com/~chris/driftnet/). The terminal shows the command `driftnet -i eth1` being executed.
- <Bsd> - Google Search - Mozilla Firefox**: A web browser window displaying the Google search results for the query "http://www.google.com/bsd". The search results show the Google Home page with the text "Search the entire web from the Google home page!" and "© 2006 Google".

The taskbar at the bottom shows the system clock as 06:48 and the network interface as eth1: Ca.

# Snort-Reply

## Unregistered HyperCam

```
$  
$ ./snort -q -v -Y -r telnet.bin
```



# Tehdit ?

- Saldırı:
- Saldırgan:
- İç Tehditler
- Dış tehditler

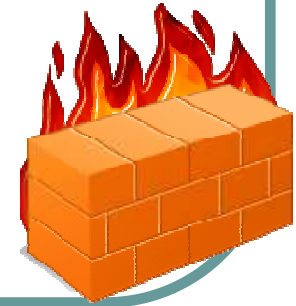




# Sınır Koruma Evrimi



- Routerler üzerine yazılan erişim kontrol listeleri(ACL)
- Güvenlik duvarlarının gelişimi
  - Durum korumasız güvenlik duvarları
  - Durum korumalı(Stateful packet inspection)
- Saldırı Tespit Sistemleri(IDS)
  - Pasif , sensor tabanlı , kompleks, false positive oranı yüksek.. Sonuç?.
- Saldırı tespit ve Engelleme (IDP) Sistemler
  - Aktif, Protokol analizi, anormallik sezinleme,



# Durum Korumalı Güvenlik duvarları ile Koruma

- Kaynak:
  - Paket nerden geliyor?
- Hedef:
- Servis:
  - Hangi servis/port için incelenecek?
- Oturum:
  - Oturum başlatan kim? Gelen paket hangi oturuma ait?
  - TCP Bayrakları bağlantı aşamasına uygun mu?..



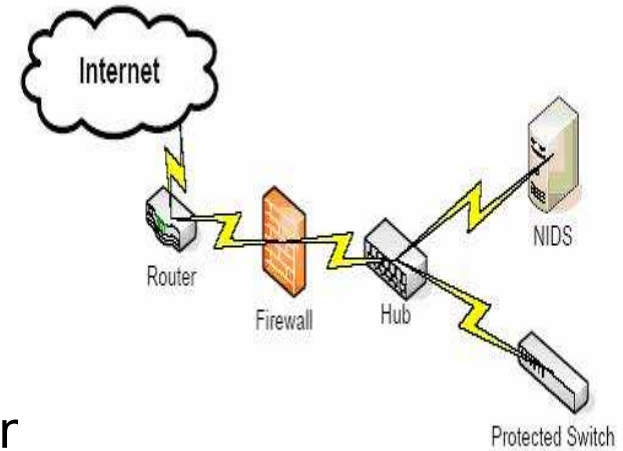
??Sonuç ??

## (N)IDS, (N)IPS, Inline, Active Response Tanımları

- IDS – Intrusion Detection System
  - Pasif Koruma
  - Active Response
  - NIDS, HIDS, WIDS, DIDS
- IPS – Intrusion Protection System
  - Aktif Koruma –Inline Sistem
  - NIPS, HIPS
- False Positive, False Negative
- Sensor, Agent, Korelasyon,

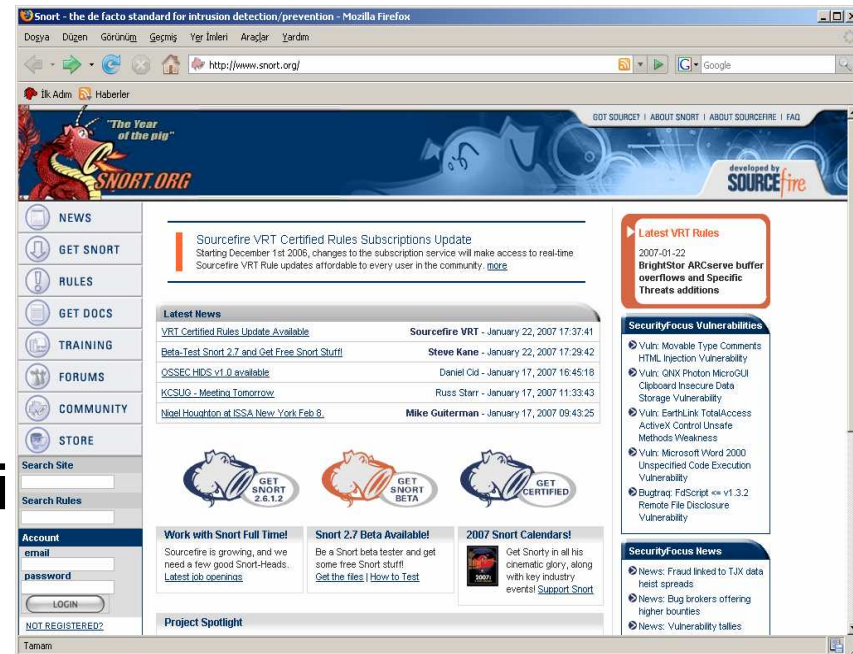
# IDS/IPS Yerleşimi

- Ağın durumuna göre yerleşim önemli
- Firewall Önü
  - Yüklü miktarda uyarı, gereksiz trafik
  - Tehditleri daha iyi belirler
- Firewall arkası
  - Sadece FW'an geçen paketler, trafik yoğun
  - Tehditleri daha az belirleyebilir.
- Switch Span portu, özel network tap cihazları(Internal)
  - Linux/BSD yüklü sağlam sunucu

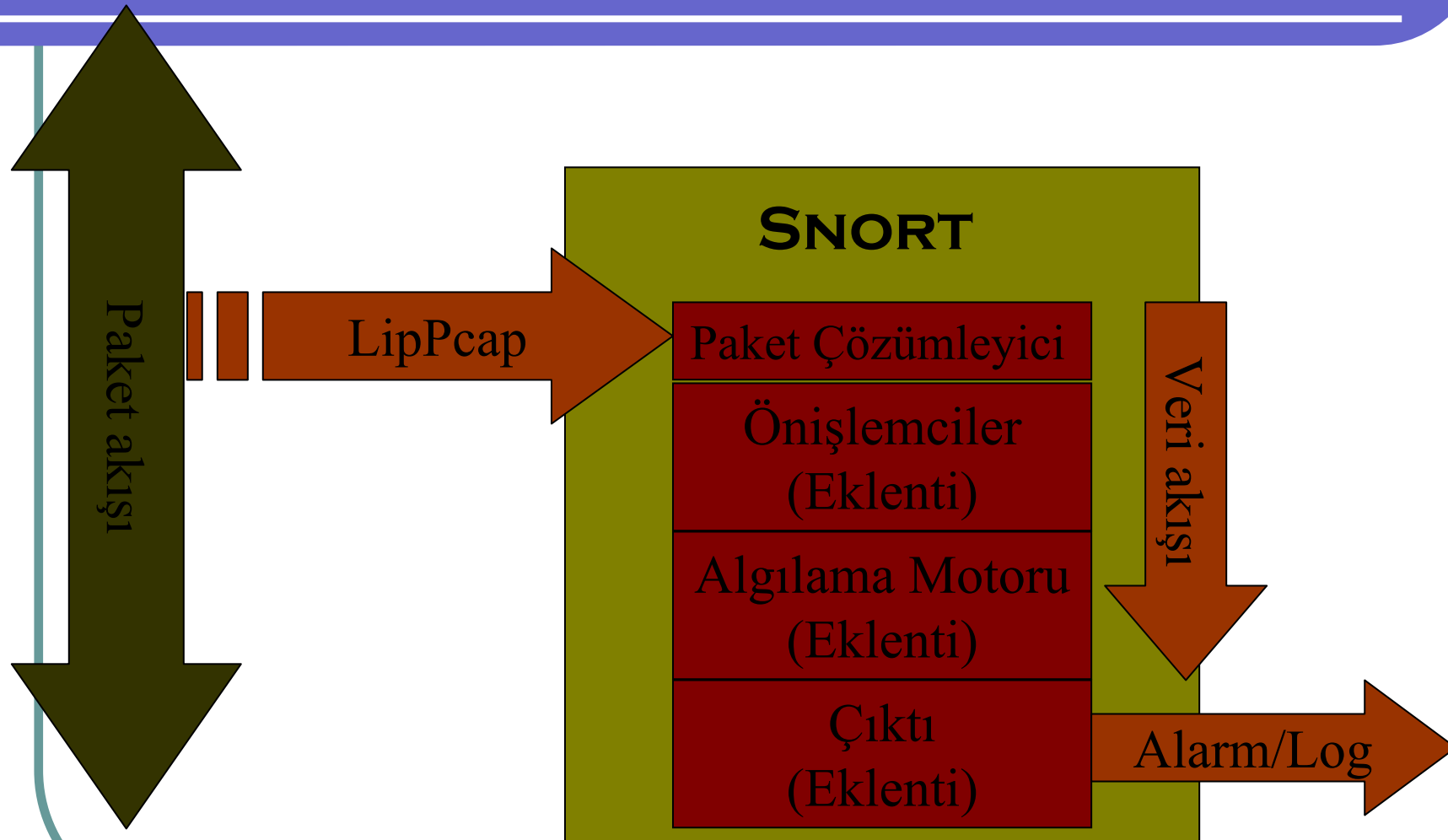


# Snort: Açık Kodlu Atak Engelleme Sistemi

- Açık Kaynak Kodlu, Özgür Lisansa Sahip
- '98 yılında hobi amaçlı başlangıç
- Günümüzde: akademik, askeri, ticari kullanım alanları
- Sniffer & Logger
- (N)IDS/(N)IPS/(N>IDP
- Forensic Analiz Aracı
- Linux/UNIX/Windows
- Stateful Packet Tracking
- Hedef tabanlı IDS özelliği



# Snort IDS Mimarisi



# Snort Bileşenleri -Detay

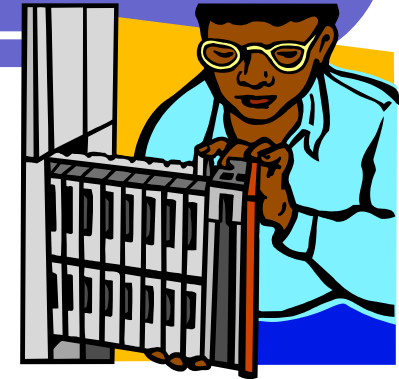
- **Libpcap** : Snort'un Ethernet kartından ham verileri almasına yarayan bileşen.
- **Decoder**: Libpcap'ın gönderdiği 2. katman verisini ayrıştırarak(2. katman için Ethernet, 802.11, 3. katman için IP, ICMP ,4. katman için tcp/udp gibi) ve bir üst katmana sunar.
- **Preprocessor**: Çözümlemiş paketleri Snort'un anlayacağı daha anlamlı parçalar haline getirir. Snort yapılandırma dosyasından aktif edilebilir ya da devre dışı bırakılabilir.. Mesela port tarama pre.'ini aktif hale getirilirse Snort port tarama işlemlerini başarı ile yakalayacaktır.
- **Detection Engine**: Snort'un kalbi olarak da nitelendirilebilecek bu bileşen paket decoder ve prep. bileşenlerinden gelen paketleri detection pluginlerini ve önceden belirlenmiş saldırı imzalarını kullanarak 4. katman ve üzerinde işleme sokar.
- **Output**: Snort tüm bu işlemler sonucu bir uyarı verir ve bu uyarıyı kaydeder. Output plugini bu uyarının nasıl olacağı ve nereye kaydedileceği konusunu yönetir. Çeşitli output pluginler: Mysql, Oracle , syslog , ikili dosya formatı ve text dosyadır





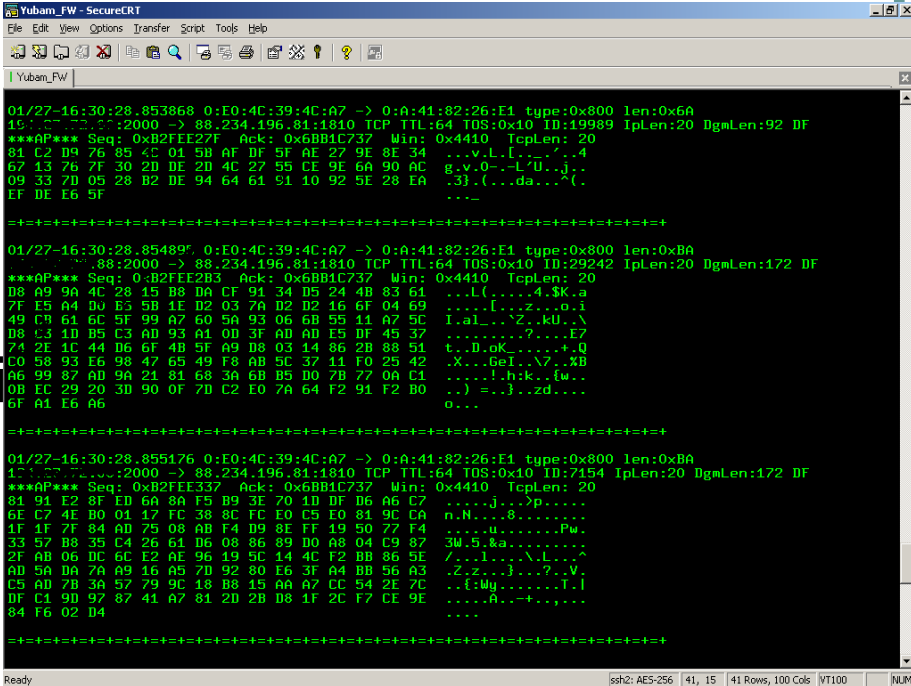
# Snort Kurulumu

- İşletim Sistemi, donanım seçimi önemli..
- Kurulum için ön gereksinimler
  - Libpcap, pcre ...
- Klasik UNIX Kurulum adımları
  - (./configure && make && make install)
  - --enable-flexresp
  - --enable-inline
  - --with-mysql
- Windows için hazır ikili paketler (WinSnort Projesi)
- **SnortVM** : Snort ,BASE, MySQL on CentOS 4.3  
Vmware imajı



# Snort Çalışma Modları -Sniffer

- Tcpump benzeri yapı
- Bpf filtreleri ile esnek kurallar yazma imkanı
- L2-L7 trafik analizi
- `./snort -v`
- L2 bilgileri için  
`./snort -v -e`
- Veri kısmının sniff edilmesi  
`./snort -v -d`



The screenshot shows a SecureCRT terminal window titled 'Yubam\_FW - SecureCRT'. The terminal displays Snort traffic analysis output for three packets. Each packet line starts with a timestamp and IP addresses, followed by protocol details and a hex dump of the packet data. The hex dump is preceded by a separator line of equals signs. The output is as follows:

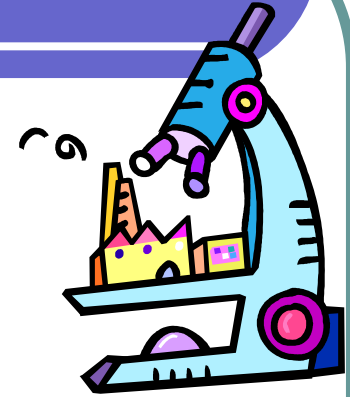
```
01/27-16:30:28.853868 0:E0:4C:39:4C:A7 -> 0:A:41:82:26:E1 type:0x800 len:0x6A
19:1:0:0:0:0:2000 -> 88.234.196.81:1810 TCP TTL:64 TOS:0x10 ID:19989 Iplen:20 DgmLen:92 DF
***AP*** Seq: 0xB2FEE27F Ack: 0x6BB1C737 Win: 0x4410 TcpLen: 20
81 C2 D9 76 85 4C 01 5B AF DF 5F AE 27 9E 8E 34 ...v.L[....'.4
67 13 76 7F 30 2D DE 2D 4C 27 55 CE 9E 6A 90 AC g.v.0--L^U..j..
09 33 7D 05 28 B2 DE 94 64 61 91 10 92 5E 28 EA .3).(....da....^(.
EF DE E6 5F .....

=====
01/27-16:30:28.854895 0:E0:4C:39:4C:A7 -> 0:A:41:82:26:E1 type:0x800 len:0xBA
19:1:0:0:0:0:2000 -> 88.234.196.81:1810 TCP TTL:64 TOS:0x10 ID:29242 Iplen:20 DgmLen:172 DF
***AP*** Seq: 0xB2FEE2B3 Ack: 0x6BB1C737 Win: 0x4410 TcpLen: 20
D8 A9 9A 4C 28 15 B8 DA CF 91 34 D5 24 4B 83 61 ...L(.....4.$K.a
7F E5 A4 D0 B3 5B 1E D2 03 7A D2 D2 16 6F 04 69 ....[....z...o..i
49 C9 61 6C 5F 99 A7 60 5A 93 06 68 55 11 A7 5C L.al...Z..kU..\\
D8 L3 1D B5 C3 AD 93 A1 0D 3F AD AD E5 DF 45 37 .....?....E7
74 2E 1C 44 D6 6F 4B 5F A9 D8 03 14 86 2B 88 51 t..D.oK.....+.Q
C0 58 93 E6 98 47 65 49 F8 AB 5C 37 11 F0 25 42 .X...GeI..\\?..xB
A6 99 87 AD 9A 21 81 68 3A 6B B5 D0 7B 77 0A C1 .....!..h:k..{w..
0B EC 29 20 3D 90 0F 7D C2 E0 7A 64 F2 91 F2 B0 ..) =..}..zd....
6F A1 E6 A6 .....o...

=====
01/27-16:30:28.855176 0:E0:4C:39:4C:A7 -> 0:A:41:82:26:E1 type:0x800 len:0xBA
19:1:0:0:0:0:2000 -> 88.234.196.81:1810 TCP TTL:64 TOS:0x10 ID:7154 Iplen:20 DgmLen:172 DF
***AP*** Seq: 0xB2FEE337 Ack: 0x6BB1C737 Win: 0x4410 TcpLen: 20
81 91 E2 8F ED 6A 8A F5 B9 3E 70 1D DF D6 A6 C7 .....j...>p.....
6E C7 4E B0 01 17 FC 38 8C FC E0 C5 E0 81 9C CA n.N....8.....
1F 1F 7F 84 AD 75 0B AD F4 D9 8E FF 19 50 77 F4 ....u.....Pw.
33 57 B8 35 C4 26 61 D6 08 86 89 D0 A8 04 C9 87 3W.5..k.....
2F AB 06 DC 6C E2 AE 96 19 5C 14 4C F2 B8 86 5E /....l...\\..L...^
AD 5A DA 7A A9 16 A5 7D 92 80 E6 3F A4 B8 56 A3 .Z..z..}...?..v.
C5 AD 7B 3A 57 79 9C 18 B8 15 AA A7 CC 54 2E 7C ..{My.....T..l
DF C1 9D 97 87 41 A7 81 2D 2B D8 1F 2C F7 CE 9E .....A..+.....
84 F6 02 D4 .....

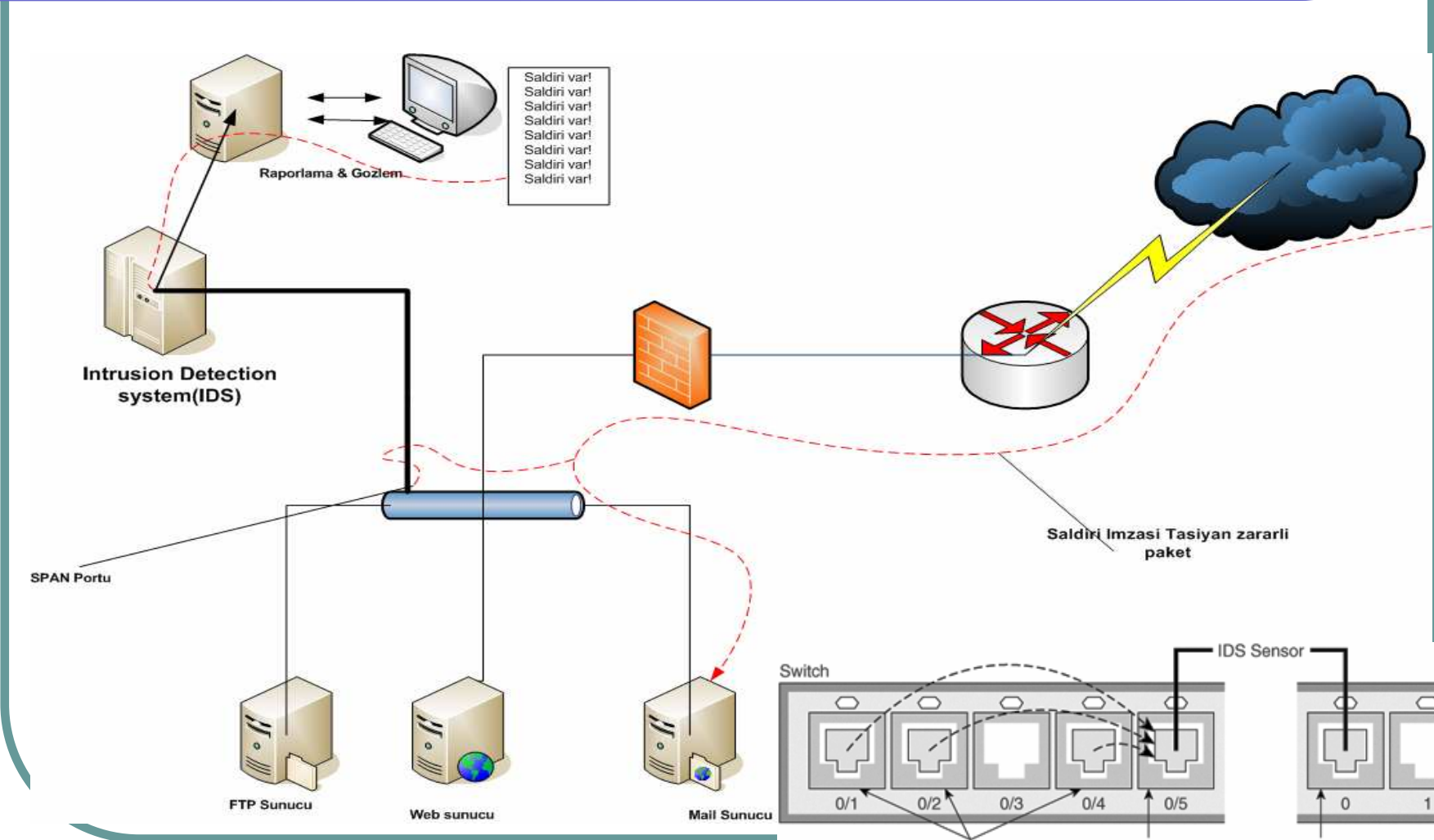
=====
```

# Snort Çalışma Modları – Packet Kaydedici

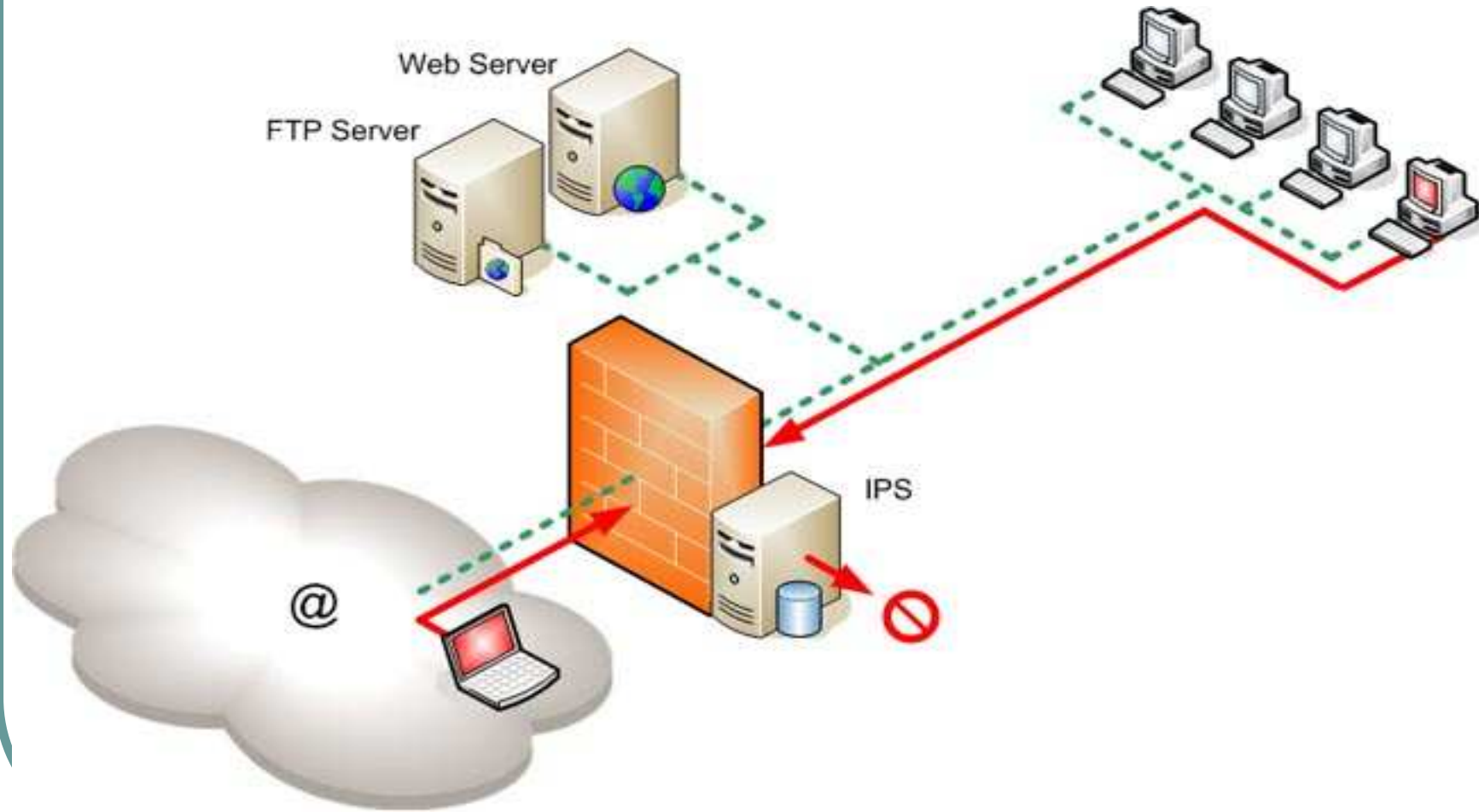


- Çeşitli formatlarda paket kaydetme
- Örnek,
  - **snort -dev -l ./log -h 192.168.0.0/24**
- Loglama seçenekleri
  - **-d** paketin veri kısmını da kaydetmek için
  - **-e** Layer2 başlıklarını kaydetmek için
  - **-l** Loglamanın hangi dizine yapılacağını belirtir)

# Snort Çalışma Modları -NIDS

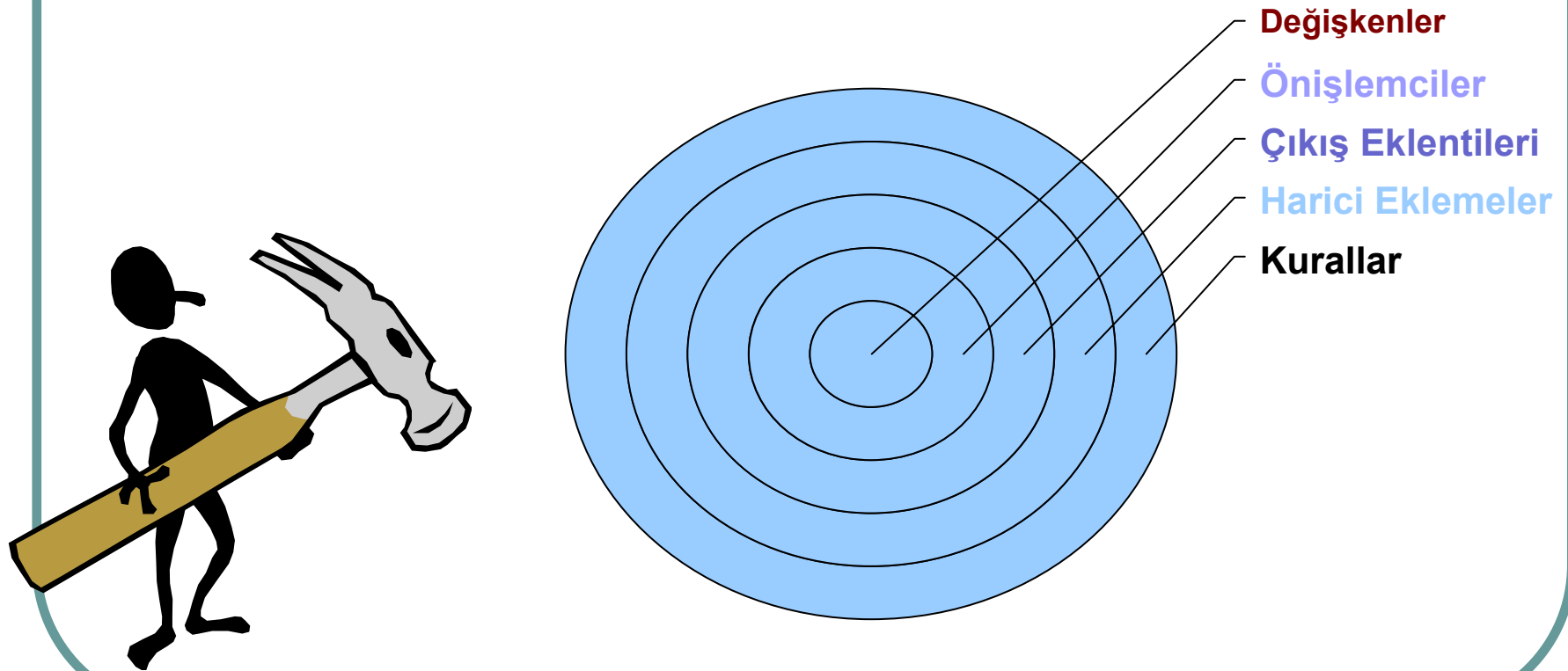


# Snort Çalışma Modları -NIPS



# Temel Snort Yapılandırması

- Tüm yapılandırma tek dosyadan: Snort.conf



# Ön işlemciler (Preprocessors)

- Packet Decode → **Preprocessors** → Detection Engine

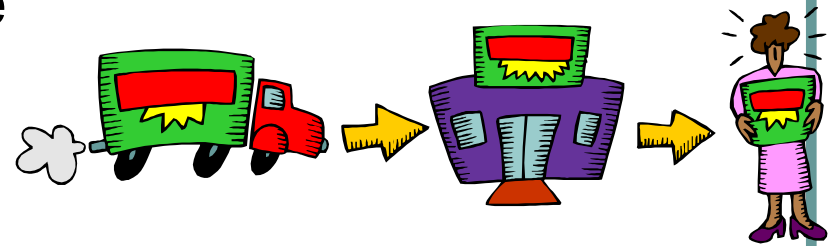
- Amaç: Paket normalleştirme

- Ip defragmentation
- Portscan Algılama
- Web trafik normalleştirme vs

- Temel Kullanımı

- `preprocessor <name>: <options>`

- Sık Kullanılan Ön işlemciler: Frag3, Stream4, Portscan, Telnet Decode, HTTP Inspect, SSH, DNS vs



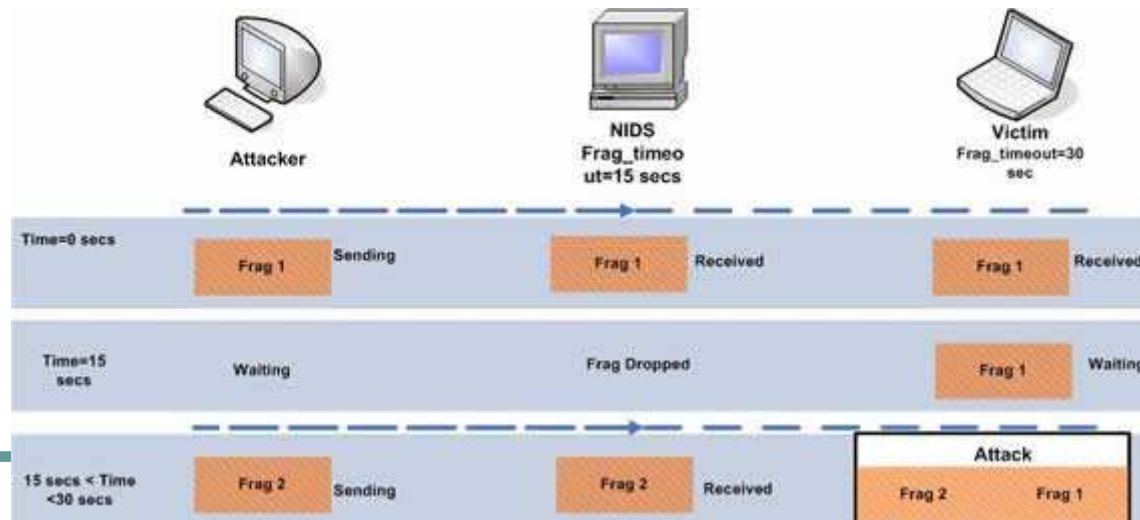


# Stream4 &Frag3 Ön işlemcileri

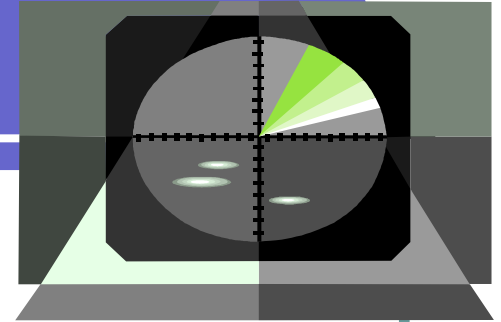


- Stream4 : Tcp Stream Reassembly
- Frag3: Hedef Tabanlı IP Parçalama modülü

```
preprocessor frag3_global: prealloc_nodes 8192
preprocessor frag3_engine: policy linux, bind_to 192.168.1.0/24
preprocessor frag3_engine: policy first, bind_to [10.1.47.0/24,172.16.8.0/24]
preprocessor frag3_engine: policy last, detect_anomalies
```



# Sfportscan Ön İşlemcisi



- Ağ tarama araçlarının korkulu rüyası
- Nmap'in gerçekleştirdiği tüm tarama türlerini yakalayabilme kapasitesi
  - TCP/UDP/IP Portscan
  - TCP/UDP/IP Decoy Portscan
  - TCP/UDP/IP Distributed Portscan ...

```
Time: 09/08-15:07:31.603880
event_id: 2
192.168.169.3 -> 192.168.169.5 (portscan) TCP Filtered Portscan
Priority Count: 0
Connection Count: 200
IP Count: 2
Scanner IP Range: 192.168.169.3:192.168.169.4
Port/Proto Count: 200
Port/Proto Range: 20:47557
```

**preprocessor sfportscan:** **proto** <protocols> **scan\_type**  
<portscan|portsweep|decoy\_portscan|distributed\_portscan|all>  
**sense\_level** <low|medium|high> **watch\_ip** <IP or IP/CIDR>  
**ignore\_scanners** <IP list> **ignore\_scanned** <IP list> **logfile** <path and filename>

# HTTP Inspect Ön işlemcisi

- HTTP protokolü için yazılmış
- HTTP başlığı ve veri alanı için normalleştirme
- Stateless Çalışıyor (paket başına kontrol)
- URL Normalleştirme
  - /foo/fake\\_dir/./bar
  - /foo/bar



```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
$HTTP_PORTS (msg:"WEB-IIS unicode directory
traversal attempt"; flow:to_server,established;
content:"/..%c0%af../"; nocase; classtype:web-
application-attack; reference:cve,CVE-2000-0884;
sid:981; rev:6;)
```

# Ftp/Telnet Ön işlemcisi

- **Genel**
- **preprocessor ftptelnet:** global inspection\_type stateful encrypted\_traffic yes check\_encrypted
- Telnet protokolü için
- **preprocessor ftptelnet:** telnet ports { 23 } normalize \ ayt\_attack\_thresh 6 detect\_anomalies
- FTP için  
preprocessor ftp\_inspect\_server: ftp server default ports { 21 }
- preprocessor ftptelnet: ftp server 10.1.1.1 ports { 21 } ftp\_cmds { XPWD XCWD }

# IDS Kurallarını Anlamak

- Oldukça Esnek kural yazma imkanı
- Hazır kuralları kullanma
  - BleedingEdge
  - SourceFire Kuralları
  - Kuralları Güncelleme -OinkMaster
- Kural = Kural Başlığı + Kural Seçenekleri
- Telnet üzerinden root kullanıcısı ile giriş algılama 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;)
```

# Kural Başlığı

- **alert tcp ! \$EXTERNAL\_NET any -> \$TELNET\_SERVERS 23**
- **Kural başlığı:** paketin nerden gelip nereye gittiğine , çeşidine(tcp, udp, icmp, ip vs) ve kurala uyan paketlerin akibetine karar verir.
- Alert/log/pass/activate/dynamic/drop/sdrop/reject.
- Tek bir IP adresi, CIDR, grupta kullanılabilir
- Analiz amaçlı Kullanım: Activate/Dynamic

```
activate tcp !$HOME_NET any -> $HOME_NET 143 (flags: PA; \
    content: "|E8C0FFFFFF|/bin"; activates: 1; \
    msg: "IMAP buffer overflow!");
dynamic tcp !$HOME_NET any -> $HOME_NET 143 (activated_by: 1; count: 50;)
```

# Kural Seçenekleri

- Detection Engine'nin kalbi sayılır
- () arasına yazılır ve birbirinden ";" ile ayrılır
- Meta-data, payload, non-payload, post-detection alanları
- Meta-data: Kural hakkında çeşitli bilgiler vermek için
  - Msg, reference, sid, priority vs
- Payload: Veri kısmında içerik kontrolü
- Non-Payload: Çeşitli protokol alanı özellikleri kontrolü
- Post-detection: Kuralın ne aksiyon alacağı

(msg:"P2P Napster Client Data"; flow:established; content:".mp3"; nocase; classtype:policy-violation; sid:564; rev:6;)



# Kural Yazma- I

- Paket veri alanında spesifik içerik tarama için kullanılır
  - content: [!] "<content string>";
- Binary(ikili) içerik için | 00 0F| kullanılır

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 53 (msg:"DNS zone transfer TCP"; flow:to\_server,established; content: "|00 00 FC|"; ... )

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 143 (msg:"IMAP login brute force attempt"; flow:to\_server,established; content:"LOGIN"; nocase;

- **Nocase:** büyük küçük harf ayrımı yapma
- **Offset:** içerik aramaya nerden başlanacağını belirtir.
- **Depth:** kaç bytelik alan aranacak

# Kural Yazma -II

- **Uricontent:** (http inspect önişlemcisi aktif olmalı)

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS  
(msg:"WEB-CGI /wwwboard/passwd.txt access"; flow:to_server,established;  
uricontent:"/wwwboard/passwd.txt"; nocase; reference:arachnids,463;  
reference:cve,CVE-1999-0953; reference:nessus,10321; reference:bugtraq,649;  
classtype:attempted-recon; sid:807; rev:7;)
```

- **PCRE Kullanımı**

```
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;)
```

# Kural Yazımı-NPD

- 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;`

# Kural Yazım Seçenekleri

- Flow: kuralın sadece belirli yöne bakmasını sağlar
  - (msg:"WEB-IIS asp-dot attempt";flow:to\_server,established;..)
- Sameip: kaynak-hedef IP aynı olması durumu

alert ip any any -> any any (msg:"BAD-TRAFFIC same SRC/DST";  
sameip; reference:cve,CVE-1999-0016;  
reference:url,www.cert.org/advisories/CA-1997-28.html;  
classtype:bad-unknown; sid:527; rev:4;)

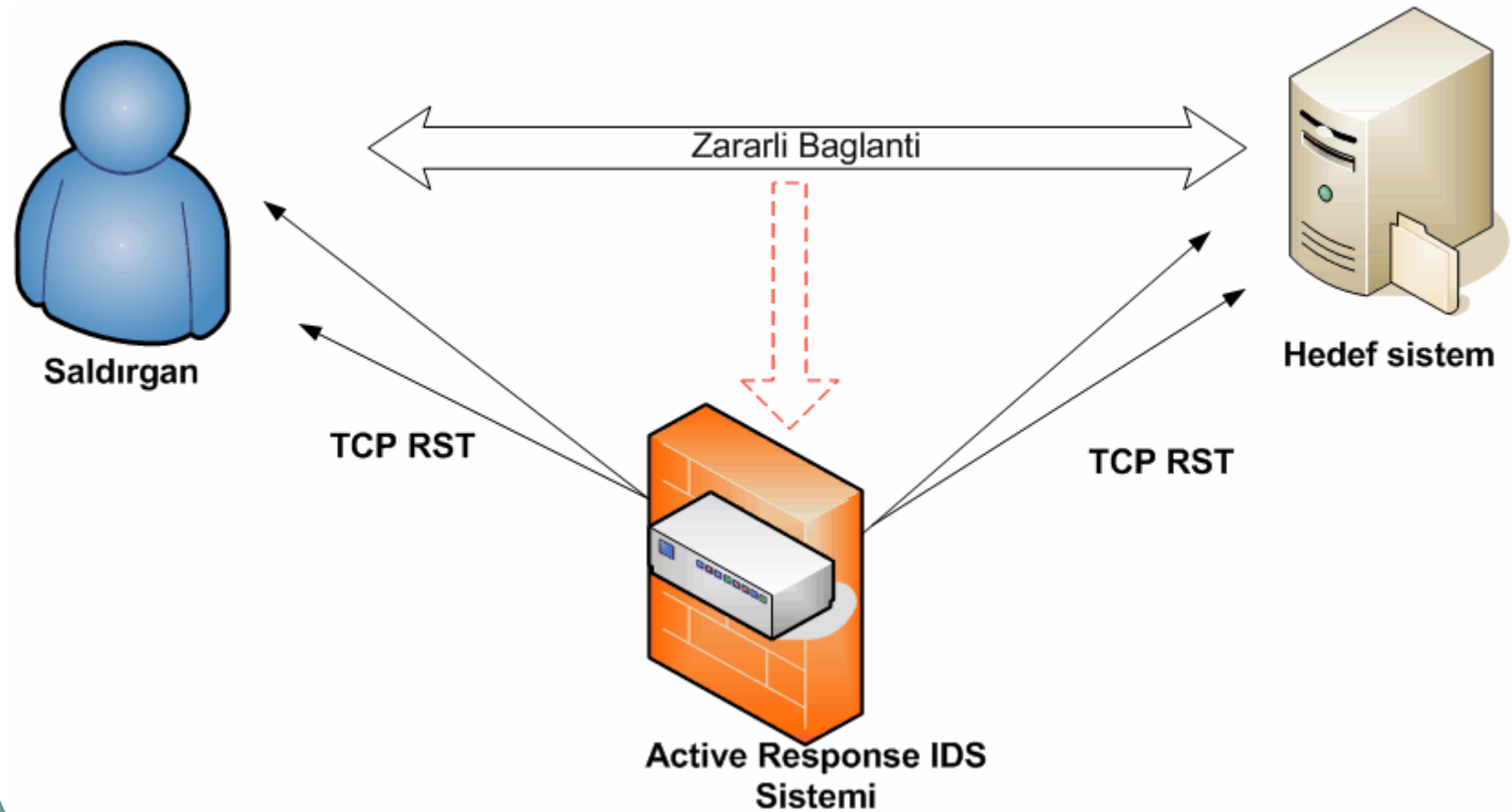
- icmp\_id, ipopts, ack, window, rpc vs

# Kural Aksiyonu Belirleme

- Session: TCP oturumlarında veri çıkartmak için kullanılır
- Sistemi yavaşlatacağı için dikkatli kullanılmalı
  - `log tcp any any <> any 23 (session:printable;)`
- React: Web kullanımında kullanıcının browserına uyarı çıkartıp bloklama yapmak için.

```
alert tcp any any <> 192.168.1.0/24 80 (content: "bad.htm"; \
msg: "Not for children!"; react: block, msg;)
```
- Resp: Bağlantı bloklama

# Aktif Yanıt sistemi Saldırı Bloklama



# Flexresp Kullanımı

- Kurulumda --enable-flexresp ile derlenmeli

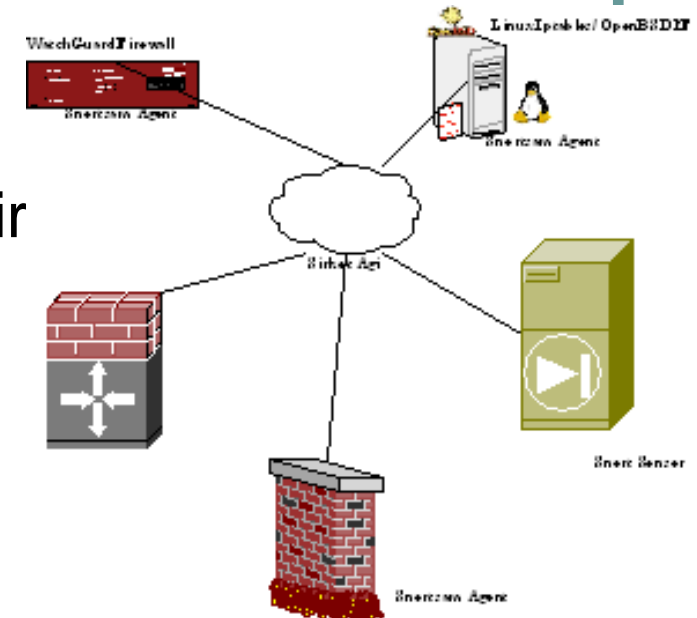
```
alert tcp $HOME_NET 2401 -> $EXTERNAL_NET any (msg:"MISC CVS invalid repository response"; flow:from_server,established; content:"error "; content:"\: no such repository"; content:"I HATE YOU"; classtype:misc-attack; sid:2009; rev:1;)
```

- Dikkatli Kullanılmalı! Dos tehlikesi
- Bloklama Seçenekleri

Option	Description
rst_snd	Send TCP-RST packets to the sending socket
rst_rcv	Send TCP-RST packets to the receiving socket
rst_all	Send TCP_RST packets in both directions
icmp_net	Send a ICMP_NET_UNREACH to the sender
icmp_host	Send a ICMP_HOST_UNREACH to the sender
icmp_port	Send a ICMP_PORT_UNREACH to the sender
icmp_all	Send all above ICMP packets to the sender

# SnortSam ile Saldırı Engelleme

- SnortSam -> Snort output plugin + Snortsam Agent
  - Active Response Özelliği != IPS
  - BeyazListe IP Desteği
  - Ajan Snort arası şifreli iletişim
  - Olaylar için loglama ve mail ile bildir
  - Zamana bağlı bloklama desteği
  - Iptables, PF, Cisco Router,
  - Checkpoint, Microsoft ISA..
- 





# SnortSam ile Bloklama

- Snort.conf

- output alert\_fwsam: firewall/idspassword

alert tcp any any -> \$HTTP\_SERVERS 80 (msg:"WEB-MISC http directory traversal"; flags: A+; content: "..\\";reference:arachnids,298; **fwsam: dest, 15 minutes;**)

# Performans

- Kötü performans=Paket Kaybı=False negatives
- Performansı Etkileyen noktalar
  - Output(çıkış) eklentileri
  - Preprocessors(Önişlemciler)
  - Rules(Kurallar)



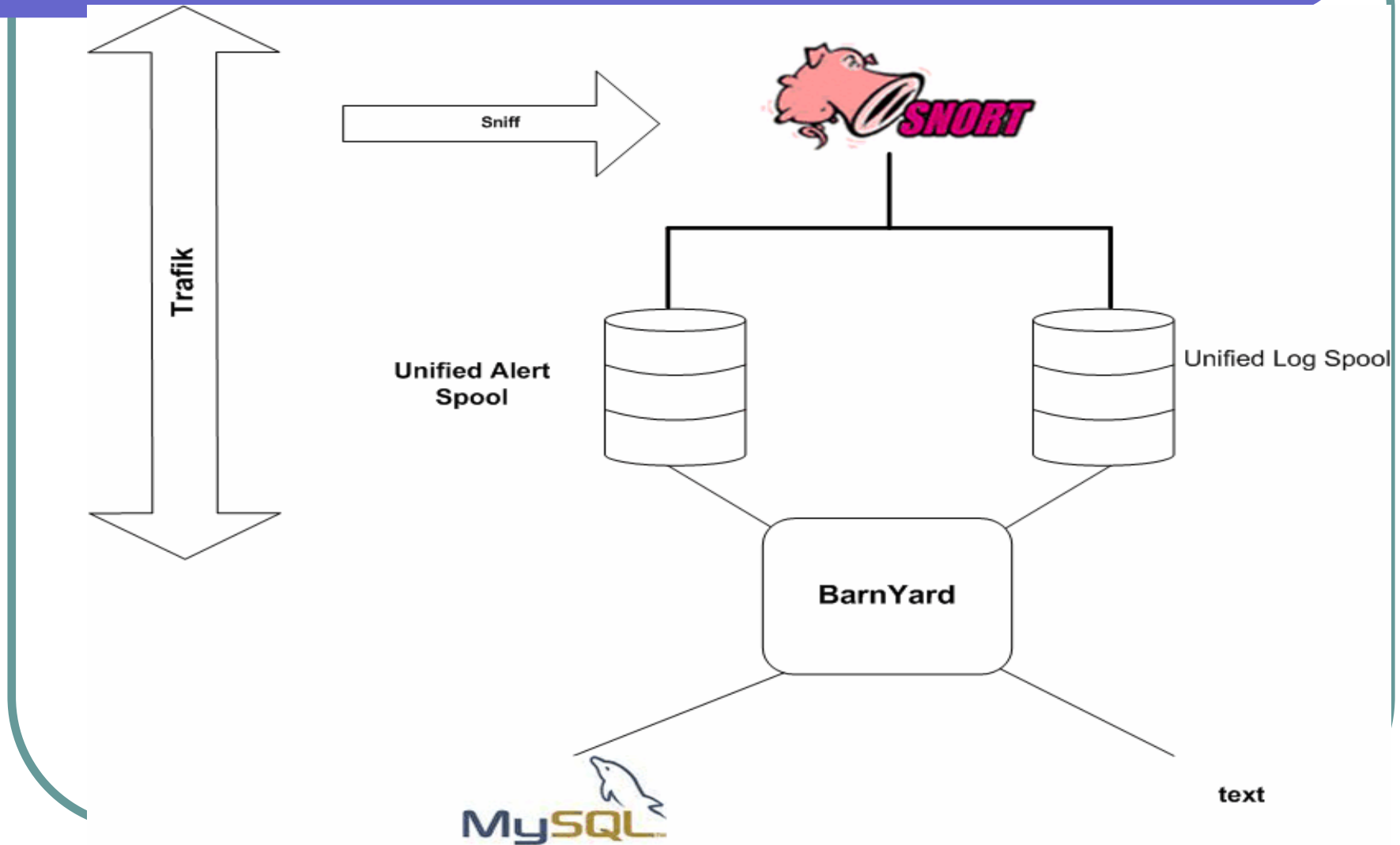
## Düşük Performanslı IDS için

- ASCII formatında Loglama
- Önişlemcilerin yanlış/eksik yapılandırılması
- Gereksiz kural fazlalığı
- Kalitesiz(yavaş) donanım kullanımı
- Çıkış plugininin performansı(database, unified)

## Yüksek Performanslı IDS için

- Binary(ikili) Loglama formatı seçimi
- Denetlenmiş kural seti
- Gereksiz Önişlemci iptali
  - Ip defragmentasyonu router yapıyorsa ids yapmamalı
- Hedef sistemlere uygun kural yazımı!
- Portscan thresholdların düşürülmesi

# Unified Output Eklentisi



# NIPS Olarak Snort

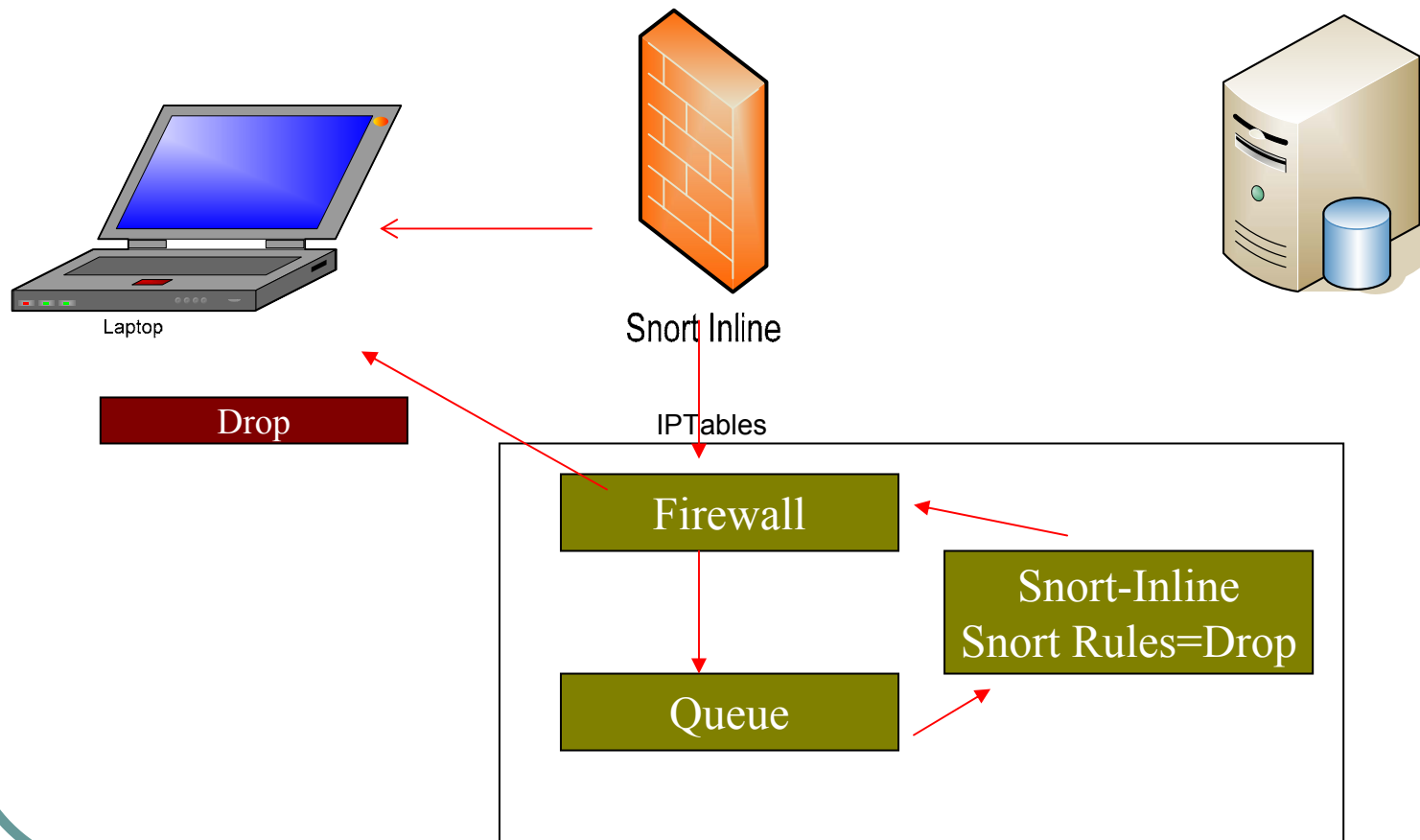
- İlk olarak Honeynet Projesinde kullanıldı
- 2. Katmanda çalışabilme özelliği
  - Linux/BSD Bridge fonksiyonu
    - `#!/usr/sbin/brctl addbr br0`
    - `#!/usr/sbin/brctl addif br0 eth0`
    - `#!/usr/sbin/brctl addif br0 eth1`
    - `#!/sbin/ifconfig br0 up`
- Saldırı engelleme, antivirus koruması , p2p engelleme, phishing vs amaçlı kullanım
- Linux -> Iptables, Libipq
- FreeBSD -> IPFW, Divert Sockets
- OpenBSD -> PQ

# Snort\_inline

- Kurulum için gereksinimler
  - Iptables, Liblpq desteği için tekrar derlenmeli(`make install-devel` )
  - Libnet Kurulumu
- Hangi Portlar için devreye alınacak
  - `iptables -D INPUT -p tcp --dport 80 -j QUEUE`
  - `iptables -D INPUT -p tcp --dport 23 -j QUEUE`

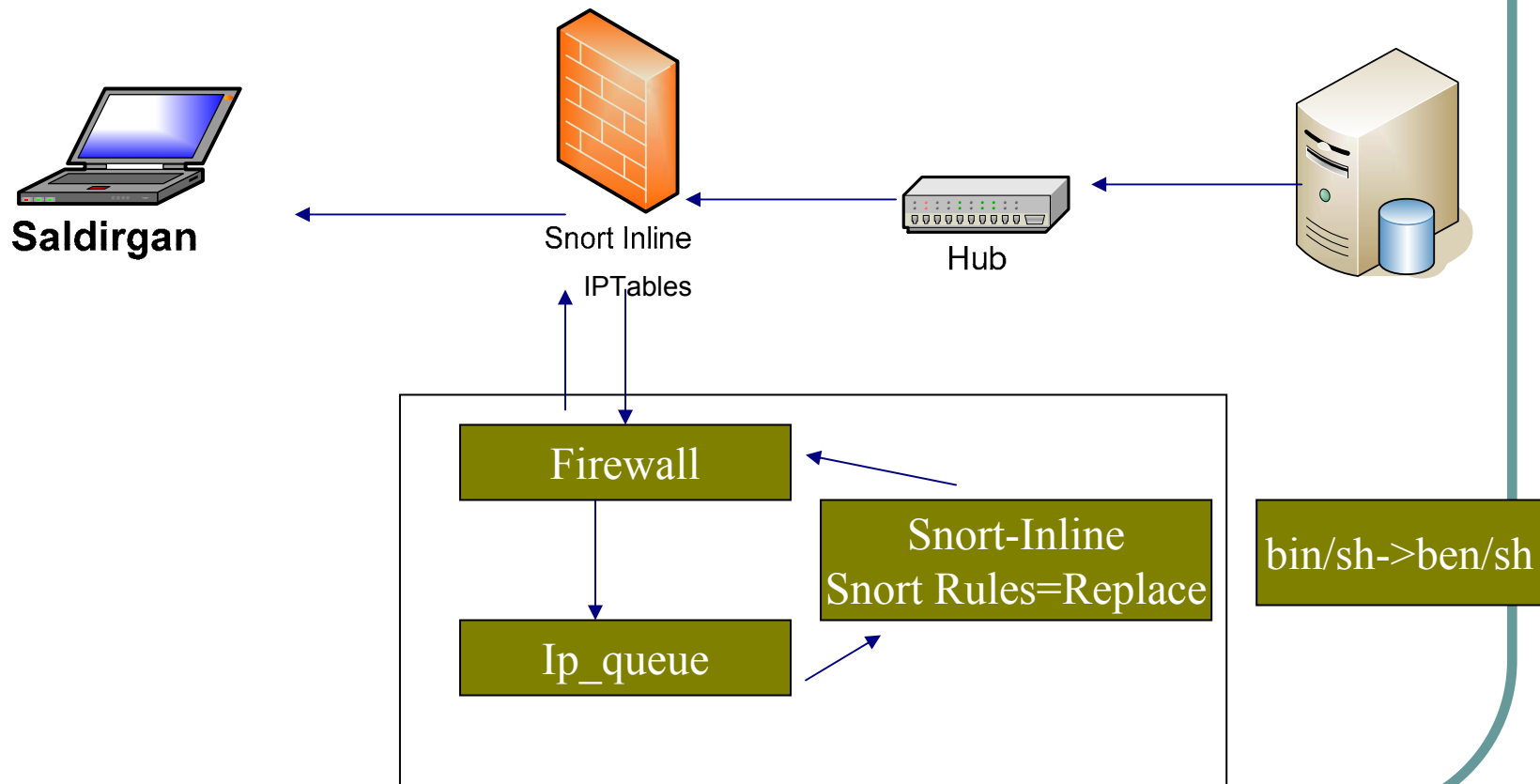
`drop tcp any any -> any 80 (classtype:attempted-user;  
msg:"Port 80 connection initiated");`

# Snort-Inline Drop Mode

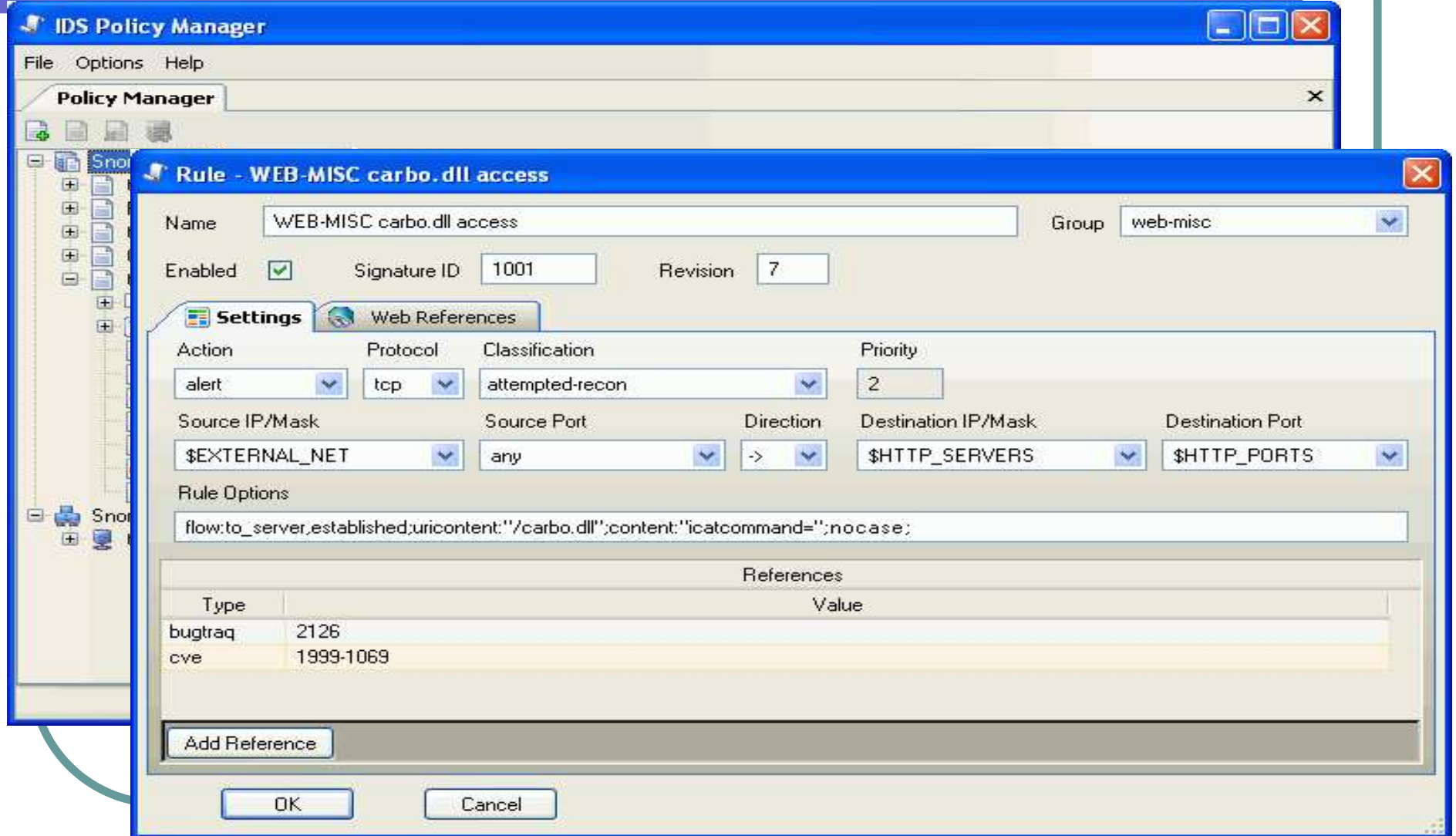




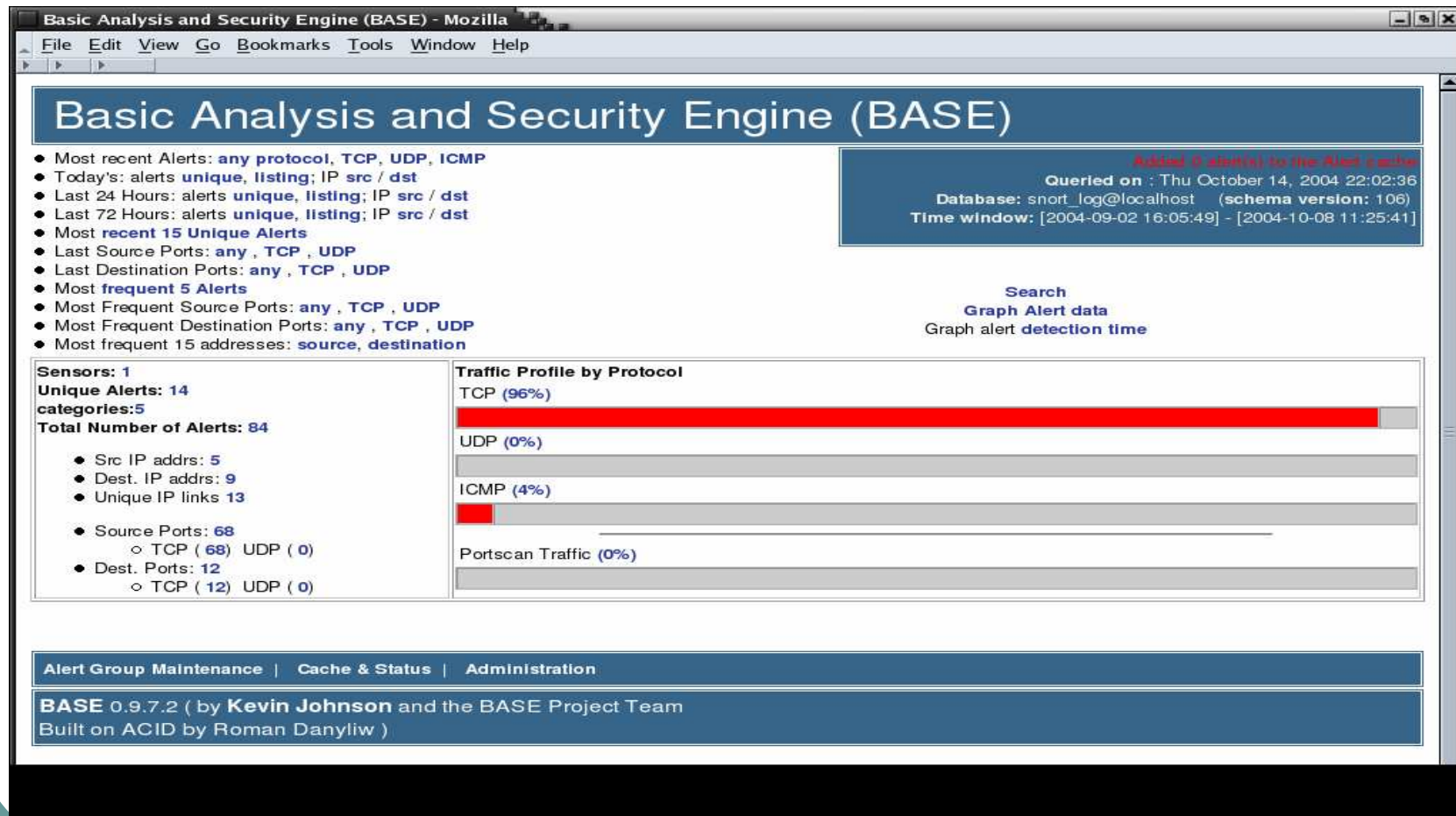
# Snort-Inline Replace Mode



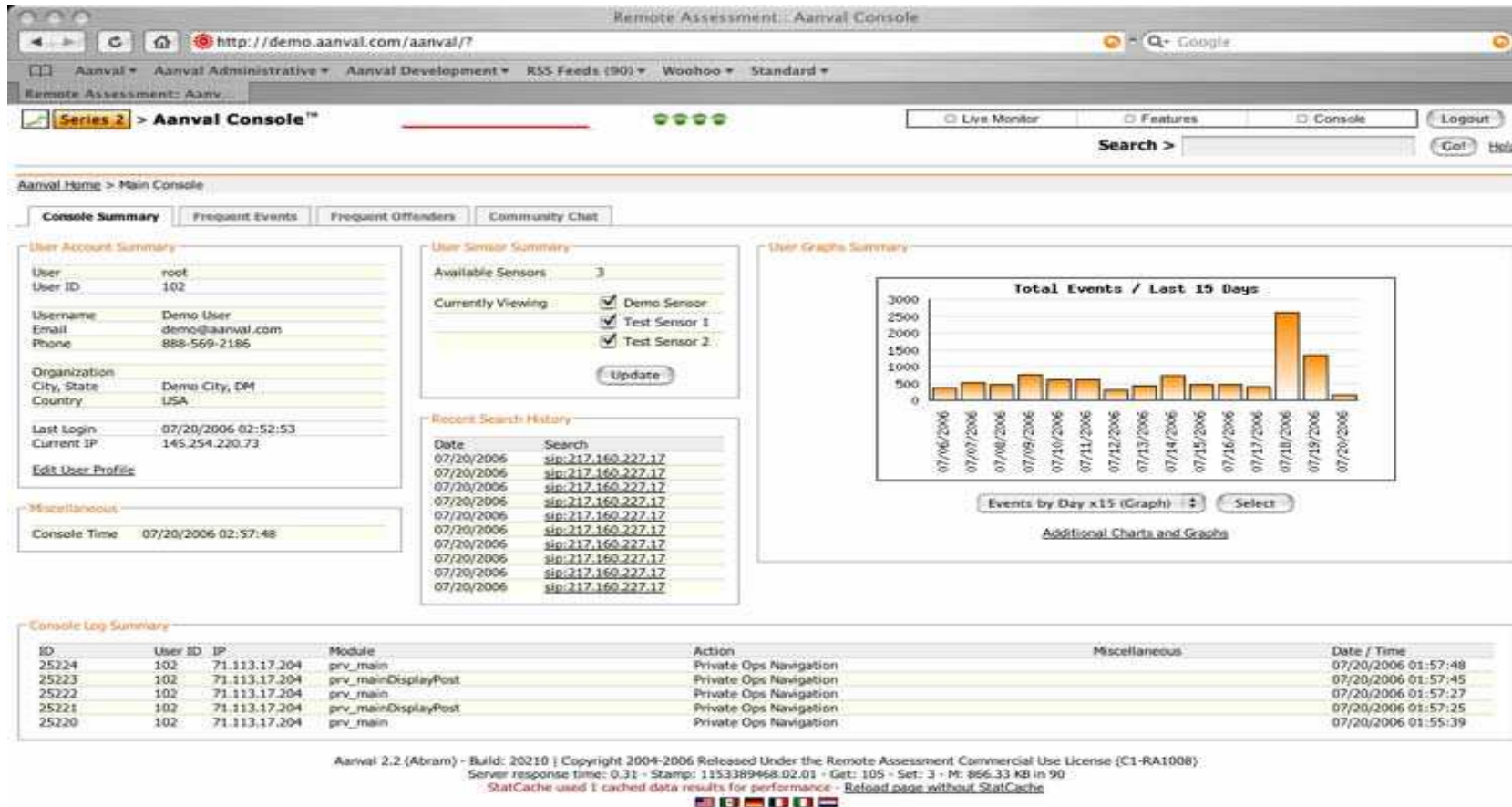
# Yönetim Araçları



# Log İzleme Araçları- BASE



# Log İzleme Araçları- Aanval



# IDS/IPS atlatma araçları ve korunma yöntemleri

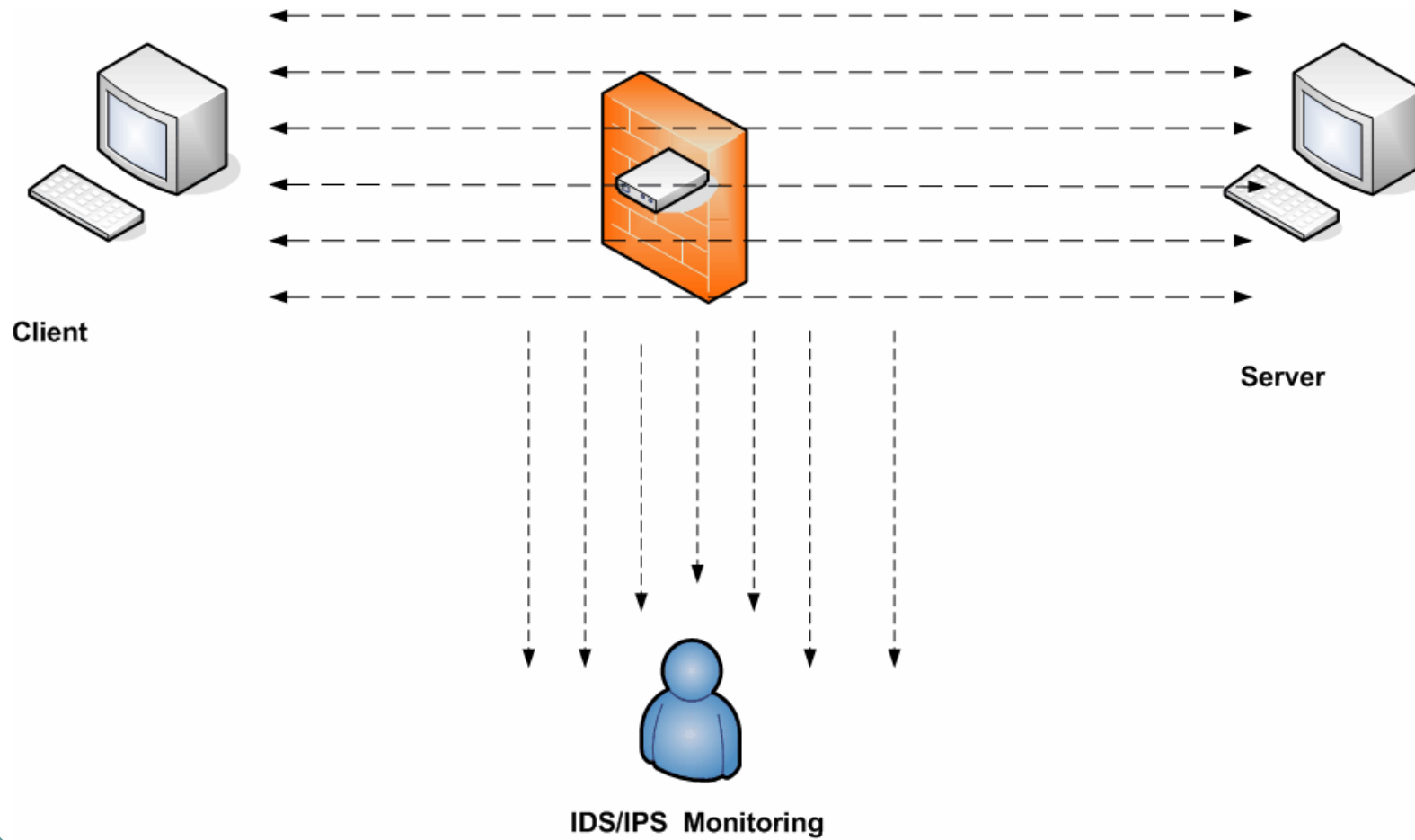
Exploit	Snort			ISS RealSecure		
	Baseline Attack	Mutated Attack	Evasion Technique	Baseline Attack	Mutated Attack	Evasion Technique
WUFTP	Detected	Evaded	Telnet ctrl seq Shellcode IP splitting	Detected	Evaded	Telnet ctrl seq Shellcode
WUIMAP	Detected	Evaded	Zero prefix Shellcode	Detected	Evaded	Junk char insertion
IISDD	Detected	Detected		Detected	Evaded	HTTP evasion
DCOMRPC	Detected	Detected		Detected	Detected	
IISUNI	Detected	Evaded	URL encoding	Detected	Evaded	HTTP evasion
ISSNSLOG	Detected	Detected		Detected	Evaded	HTTP evasion
ISSISAPI	Detected	Detected		Detected	Evaded	HTTP evasion
WSFTP	Detected	Evaded	Telnet ctrl seq IP splitting	Detected	Evaded	Telnet ctrl seq
SSLMSKEY	Detected	Evaded	SSL Null record	Detected	Evaded	SSL Null record
HTTPCNK	Detected	Evaded	HTTP evasion	Detected	Evaded	HTTP evasion

**Black Hat Briefings**

# IDS/IPS Testleri

- IDS/IPS fonksiyonlarını denetleme
  - Performans, kural seti, alarm mekanizması
- Sonuçlar..
  - False positive oranı
  - False negative oranı
- Test Araçları:
  - Fragroute, ftester, Metasploit, Nessus, Nmap, Tomahawk, idswakeup

# İstemci-Sunucu IDS Test Yapısı





# Ftester – IDS Test Aracı

- İstemci-sunucu Mimarisi(ftest- ftestd)
- Firewall Testleri
- IDS Testleri
- IP Fragmentation / IP Spoofing
- IDS Atlatma teknikleri
- Snort Kurallarını kullanabilme yeteneği



---

```
ids-conn=192.168.0.10:23:10.1.7.1:1025:PA:TCP:0:to su root
ids-conn=192.168.0.10:1025:10.1.7.1:80:PA:TCP:0:cmd.exe
ids-conn=192.168.0.10:1026:10.1.7.1:80:PA:TCP:0:ftp.exe
insert /etc/snort/exploit.rules 192.168.0.10 10.1.7.1 0
insert-conn /etc/snort/web-misc.rules 192.168.0.10 10.1.7.1 0
```

----

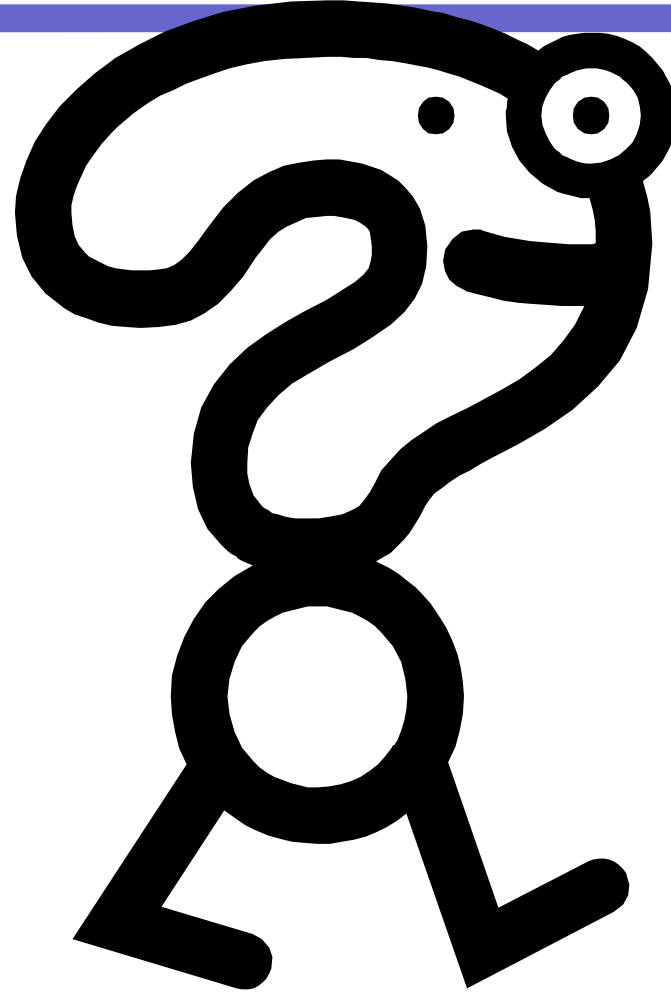


# !Sonuc

- Eğitim Şart ;-)
- Türkiye Güvenlik eğitimleri
- Kitap, Belge, Yayınlar..
  - Açık Akademi Yayınları – Güvenlik Kitapları
    - Ağ güvenliği ipucları
    - TCP/IP Güvenliği
- Olympos Security([www.olympus.org](http://www.olympus.org))
- [www.EnderUNIX.org](http://www.EnderUNIX.org)
- <http://netsec.huzeyfe.net> – Netsec Listesi



# Sorularınız



**Teşekkürler..**