

Yıl 2010...





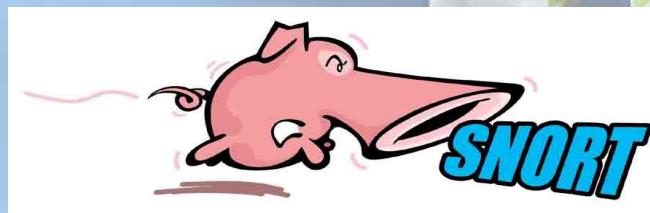
Açık Kaynak kodlu Yazılımlarla Trafik Analizi, Saldırı Tespiti Ve Engelleme Sistemleri

Huzeyfe ÖNAL

EnderUNIX Yazılım Geliştirme Takımı

huzeyfe@EnderUNIX.org

<http://www.enderunix.org/huzeyfe>

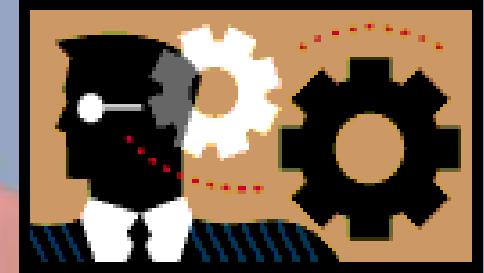


Sunum Planı

- Açık Kod Trafik Analiz Araçları
- Saldırı Tespit ve Engellemeye 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

- İletisim == Ağ Trafigi == paket
- Ne işe yarar
 - Bilinmeyen Protokol Analizi
 - Ağ trafigi başarımı
 - Anormal trafik gözleme
 - Firewall/IDS/IPS altyapısı..
- TCP, UDP Paketleri
- Protokoller
 - SMTP, FTP, P2P trafigi nasıl ayırt edilir
 - Linux L7-filter projesi
- Bilişim suçları için adli analiz imkanı

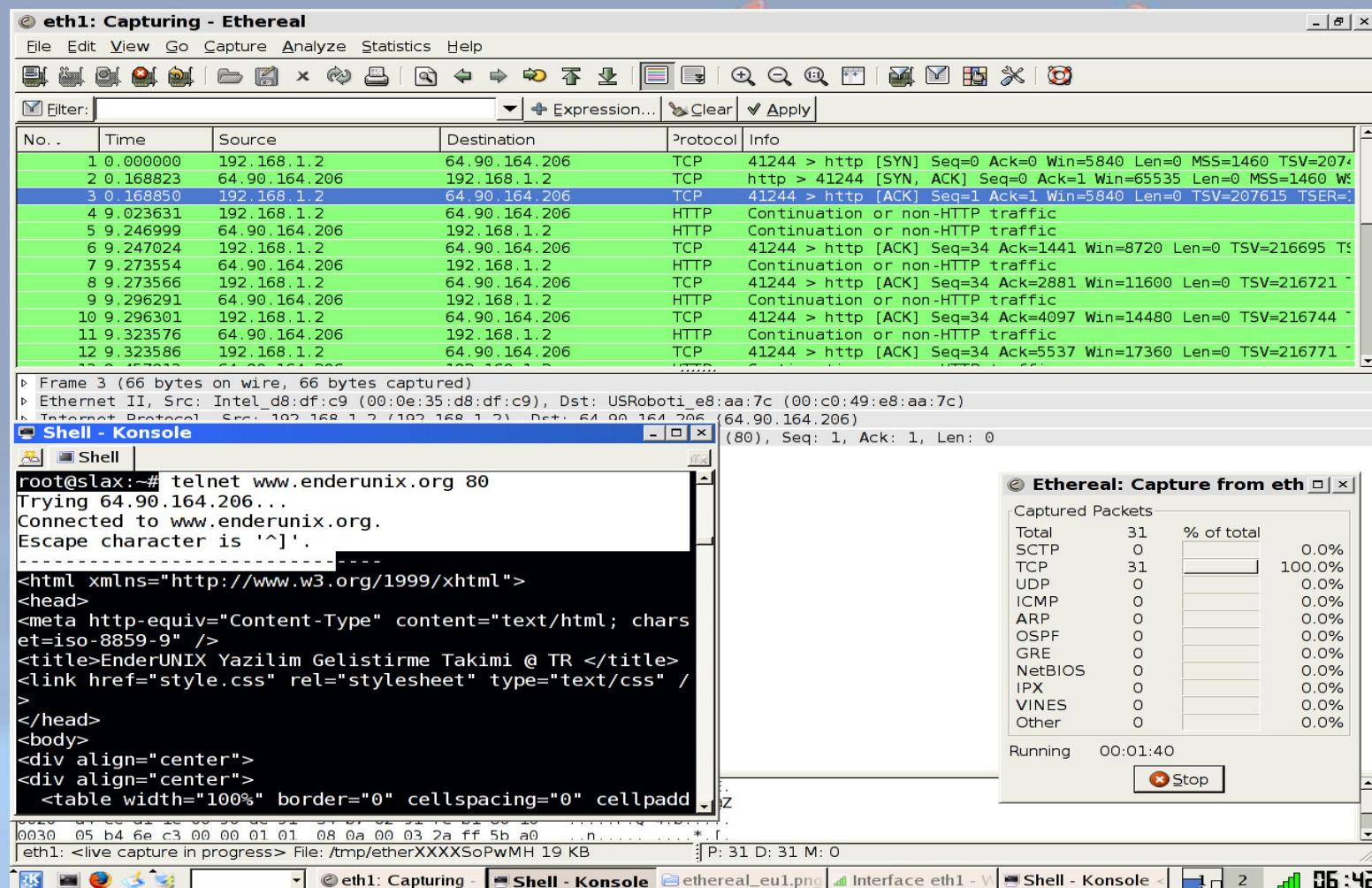


tcpdump

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



WireShark/Ethereal



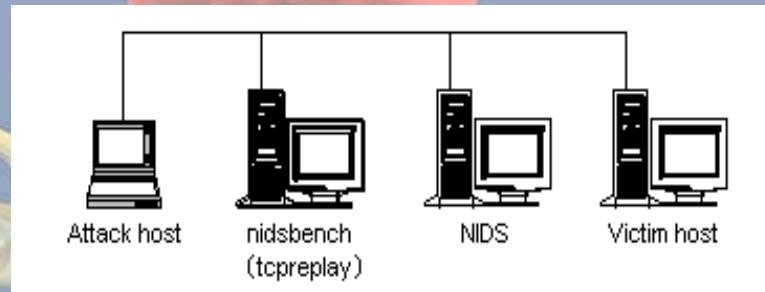
Tcpreplay

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

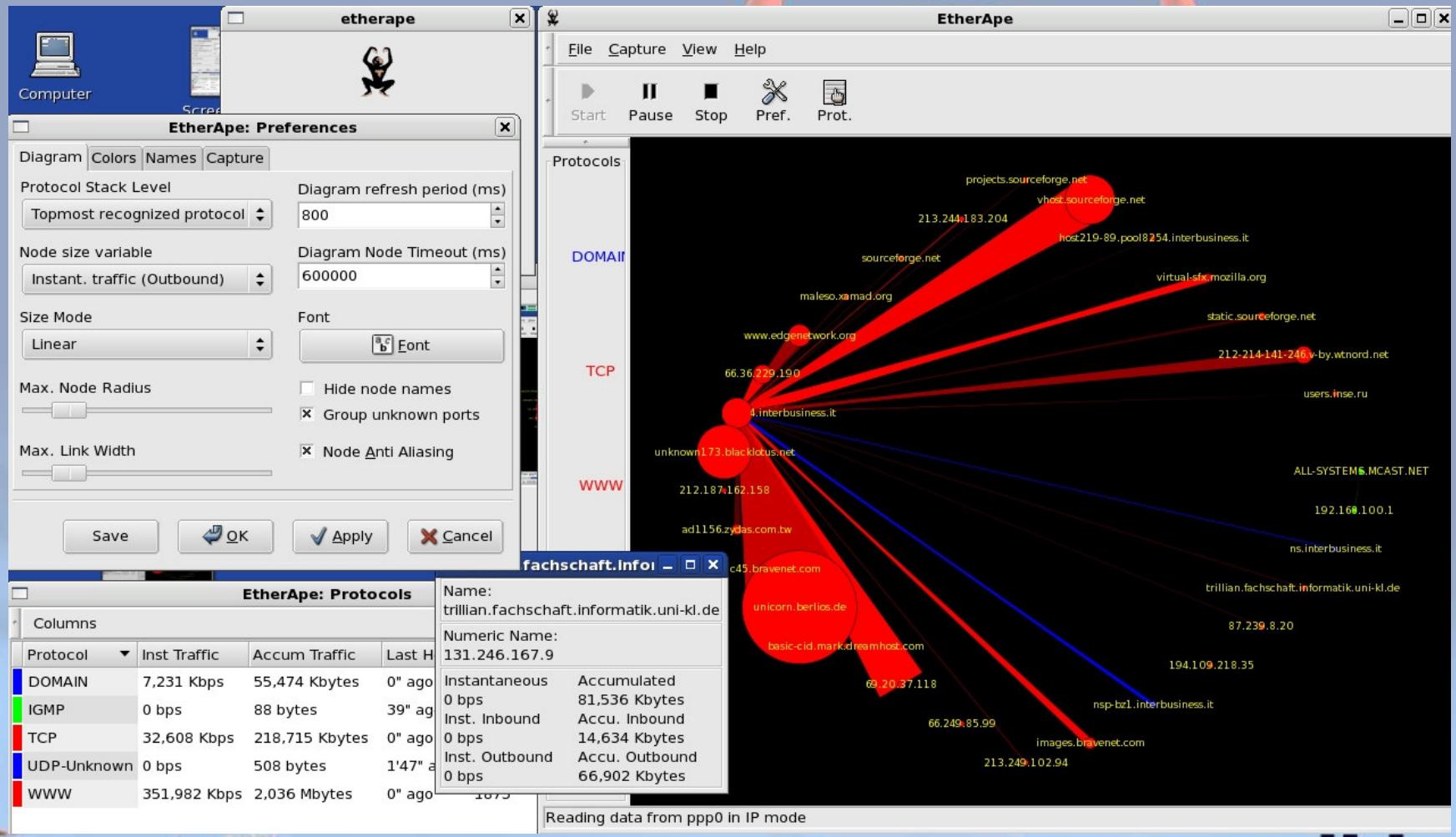
```
# tcpreplay -i r10 for_ab
```

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

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



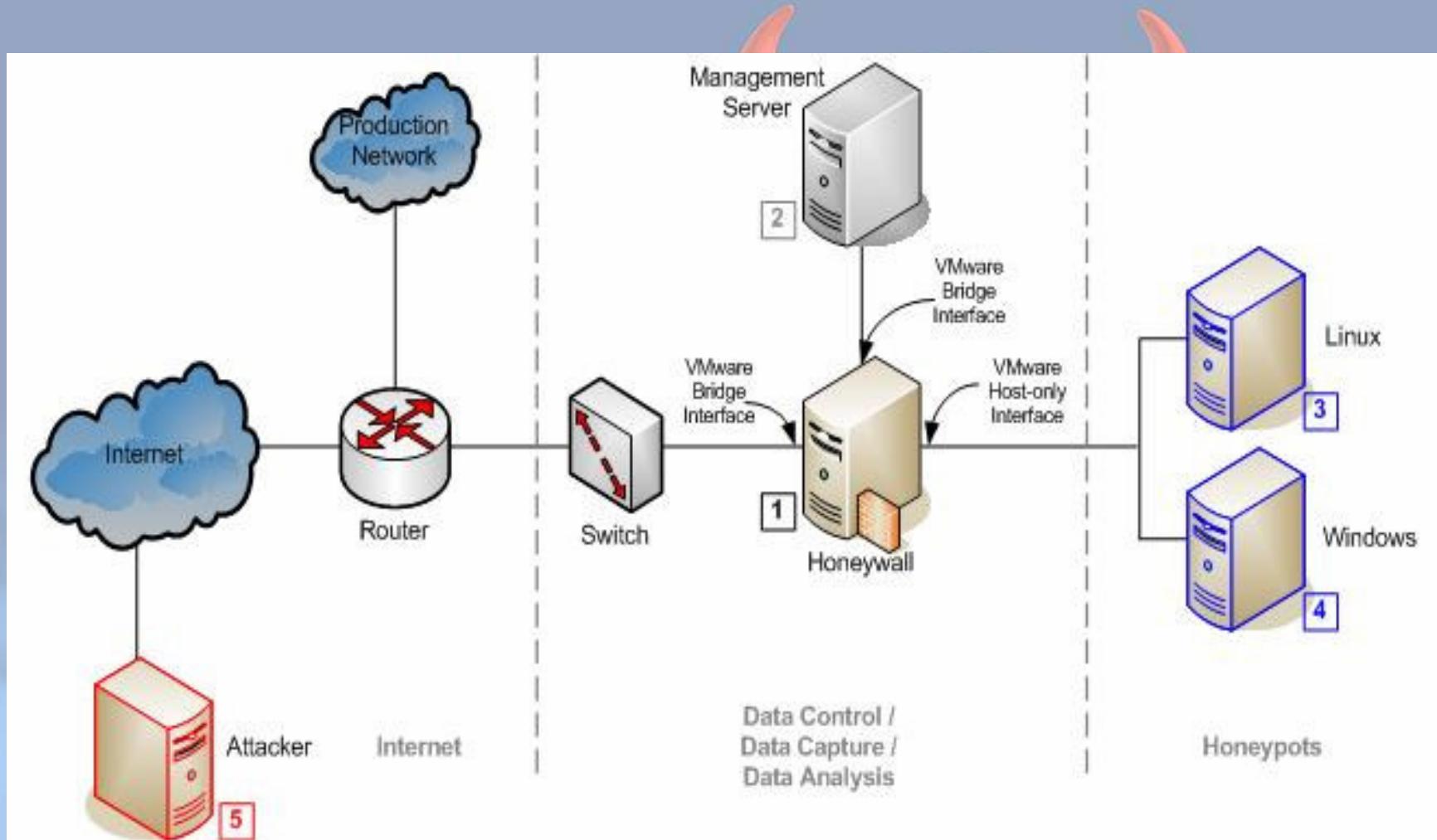
Etherape



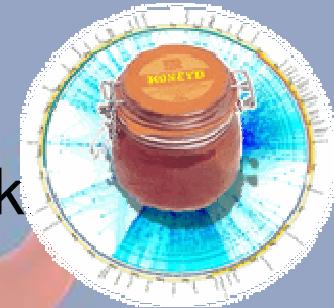
Tuzak Sistemler

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

Basit bir HoneyPot



Honeyd



- Linux/FreeBSD/OpenBSD/Windows'u destek
- Ağdaki boş IP adreslerini kullanabilir
 - Arpd cevap donulmeyen ipler için mac adresi yayımlar
- Eşzamanlı İstenilen sayıda İşletim sistemi, servis simülasyonu
- 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



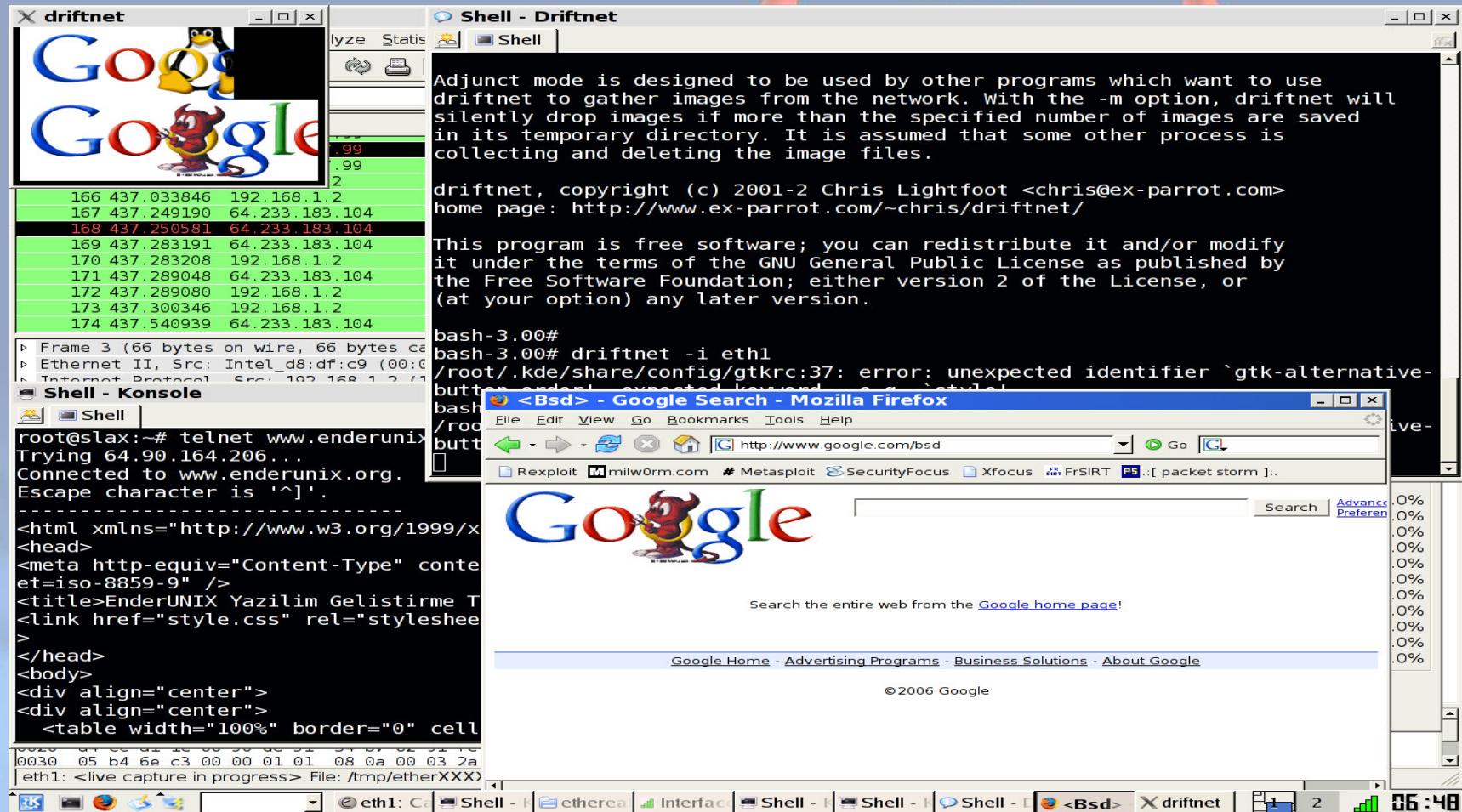
```
FreeBSD - SecureCRT
File Edit View Options Transfer Script Tools Help
[OpenBSD FW] [OpenBSD FW (1)] [YubamFW_withVPN] [FreeBSD]
[root@test /tmp/honeyd-1.5b]# honeyd -p nmap.prints -f honeyd.conf -l logfile.log 10.1. .252
Honeyd V1.5b Copyright (c) 2002-2004 Niels Provos
honeyd[29054]: started with -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]#
```

Data carving



- Ham veriden orijinal veri elde etme yöntemi
- Ağ trafiginizde 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 kaydettigim trafigi okutuyoruz, sonuc?
- **\$perl chaosreader0.94 enderunix**
- Araçlar
 - Chaos Reader, tcpflow, Driftnet..

Driftnet Kullanımı



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 sezginleme,

Durum Korumalı Güvenlik duvarları ile Koruma

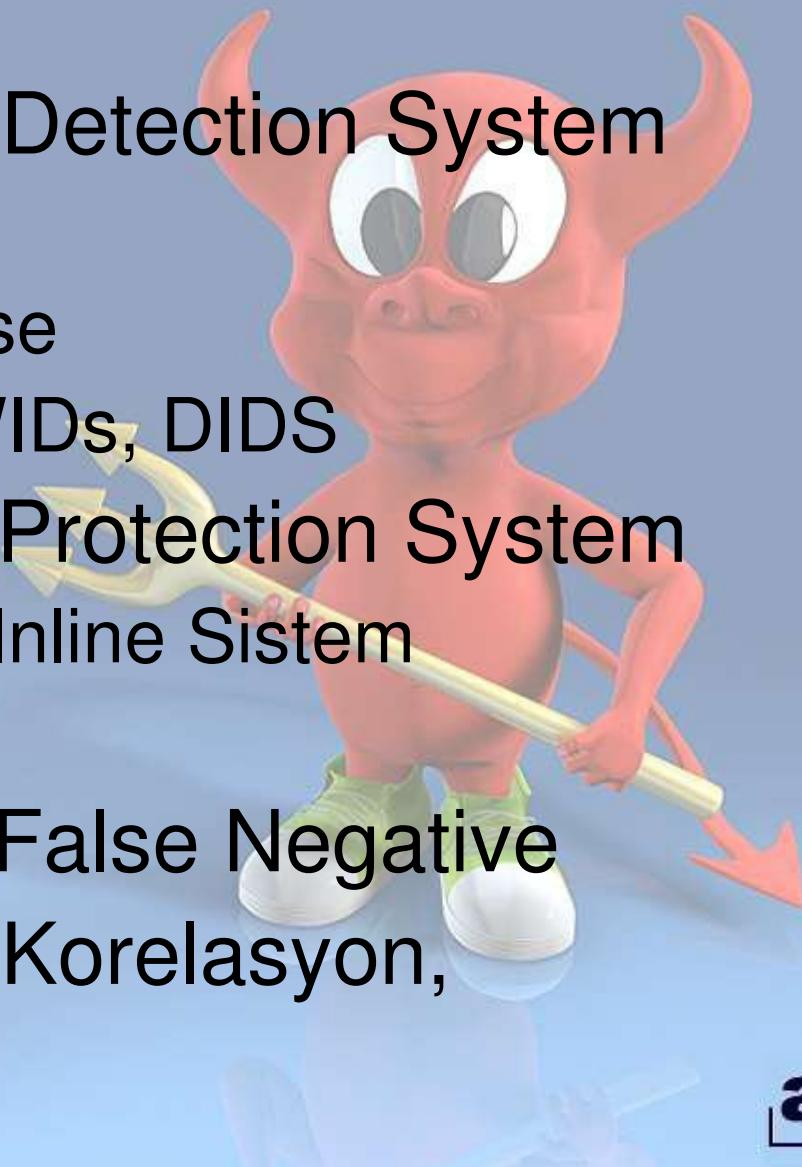
- Kaynak:
 - Paket nerden geliyor?
- Hedefe:
 - Nereye gidiyor?
- Servis:
 - Hangi servis/port için incelenecek?
- Oturum:
 - Oturum başlatan kim? Gelen paket hangi oturuma ait?
 - TCP Bayrakları bağlantı aşamasına uygun mu?..



??Sonuç ??

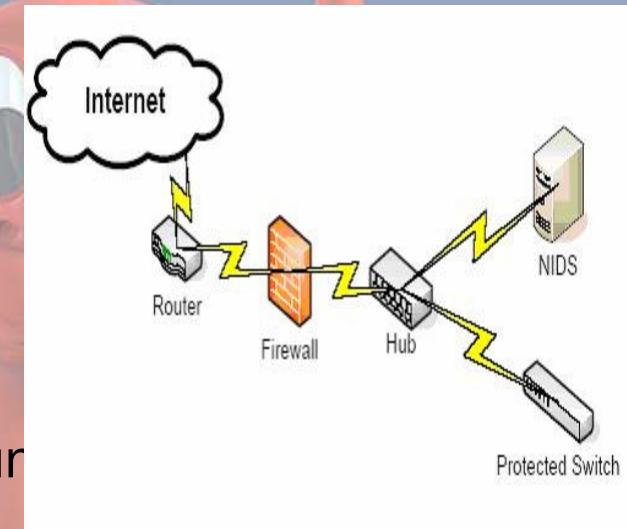
(N)IDS, (N)IPS, Inline, Active Response Tanımları

- 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,



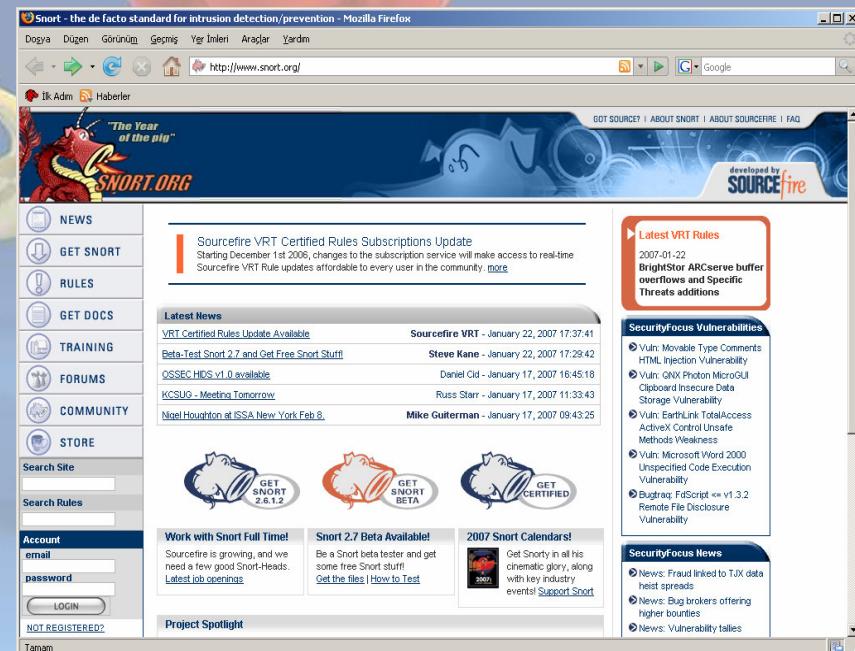
IDS/IPS Yerleşimi

- 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

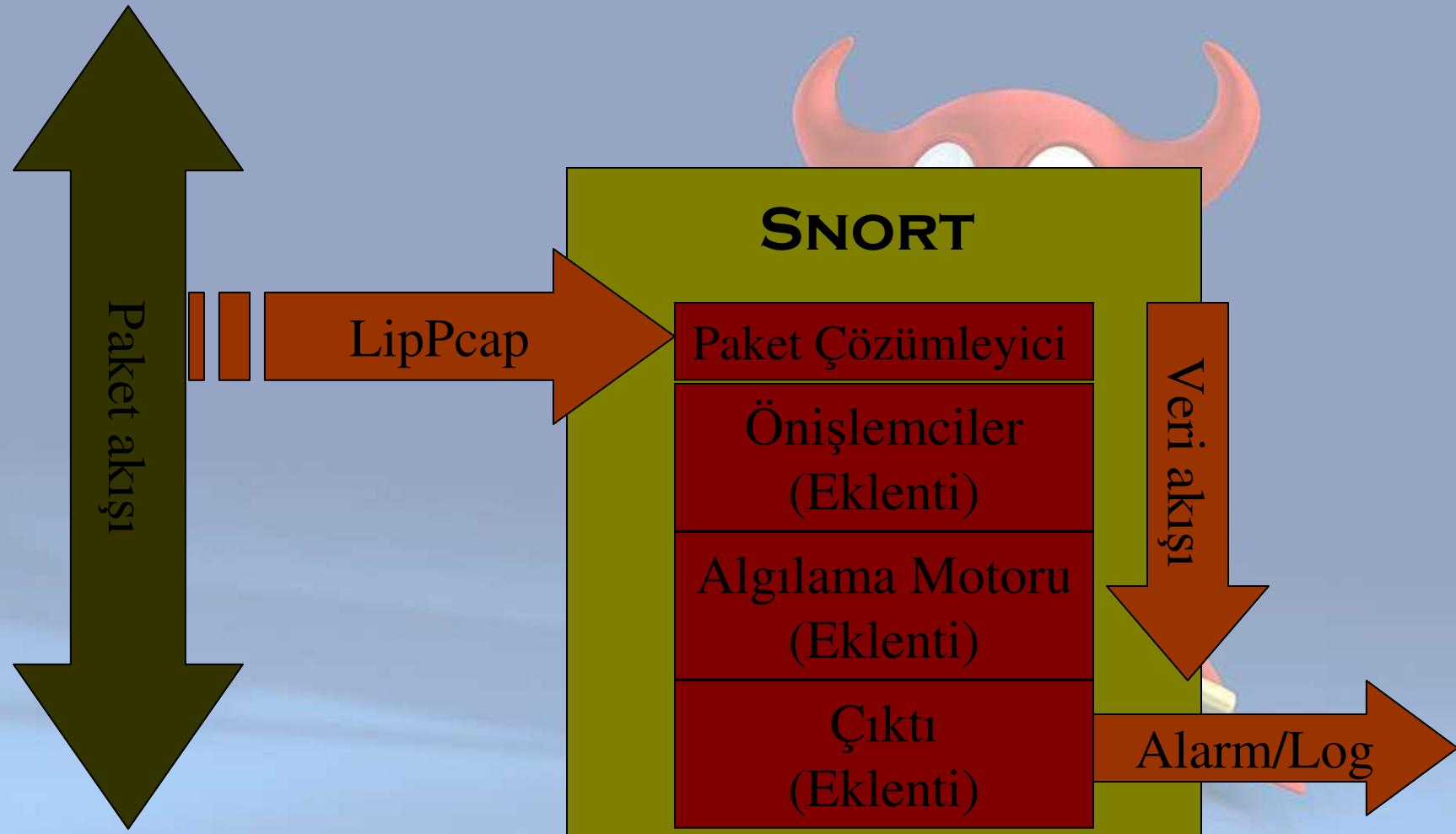


Snort: Açık Kodlu Atak Engellemeye Sistemi

- 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 ayırtırarak(2. katman için Ethernet, 802.11, 3. katman için IP, ICMP ,4. katman için tcp/udp gibi) ve bir üst katmana sunar.
- **Preprocessor**: Çözümlenmiş 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 pluginı 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

- Tcpdump benzeri yapı
 - Bpf filtreleri ile esnek kurallar yazma imkanı
 - L2-L7 trafik analizi
 - ./snort -v
 - L2 bilgileri için

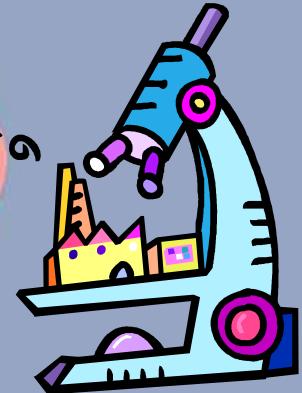
./snort -v -e

- Veri kısmının sniff edilmesi

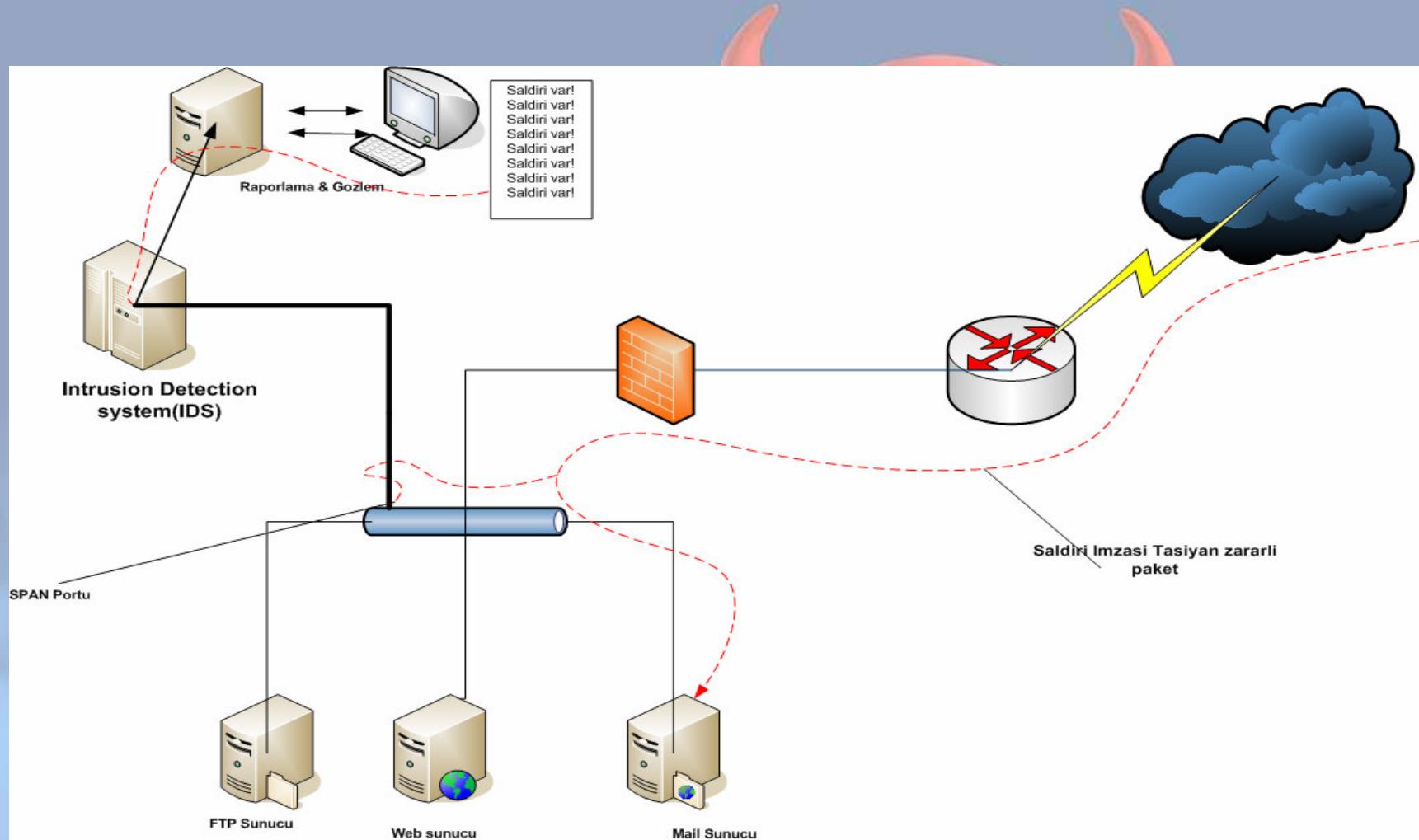
./snort -v -d

Snort Çalışma Modları – Packet Kaydedici

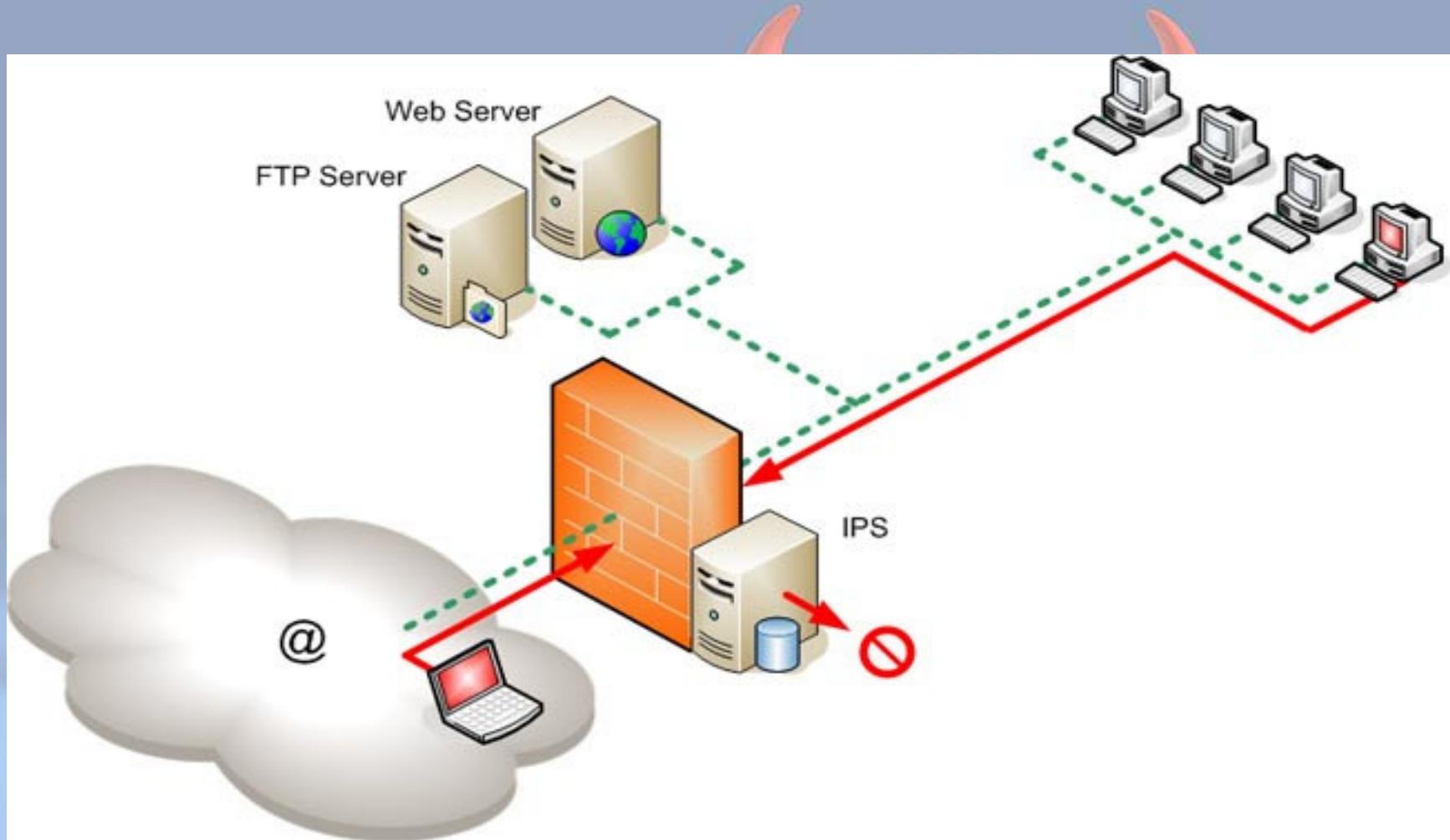
- Çeşitli formatlarda paket kaydetme
- Örnek,
 - **snort -dev -l ./log -h 192.168.0.0/24**
- Loglama seçenekleri
 - **-d** paketin veri kısmını da kaydetmek için
 - **-e** Layer2 başlıklarını kaydetmek için
 - **-I** Loglamanın hangi dizine yapılacağını belirtir)



Snort Çalışma Modları -NIDS

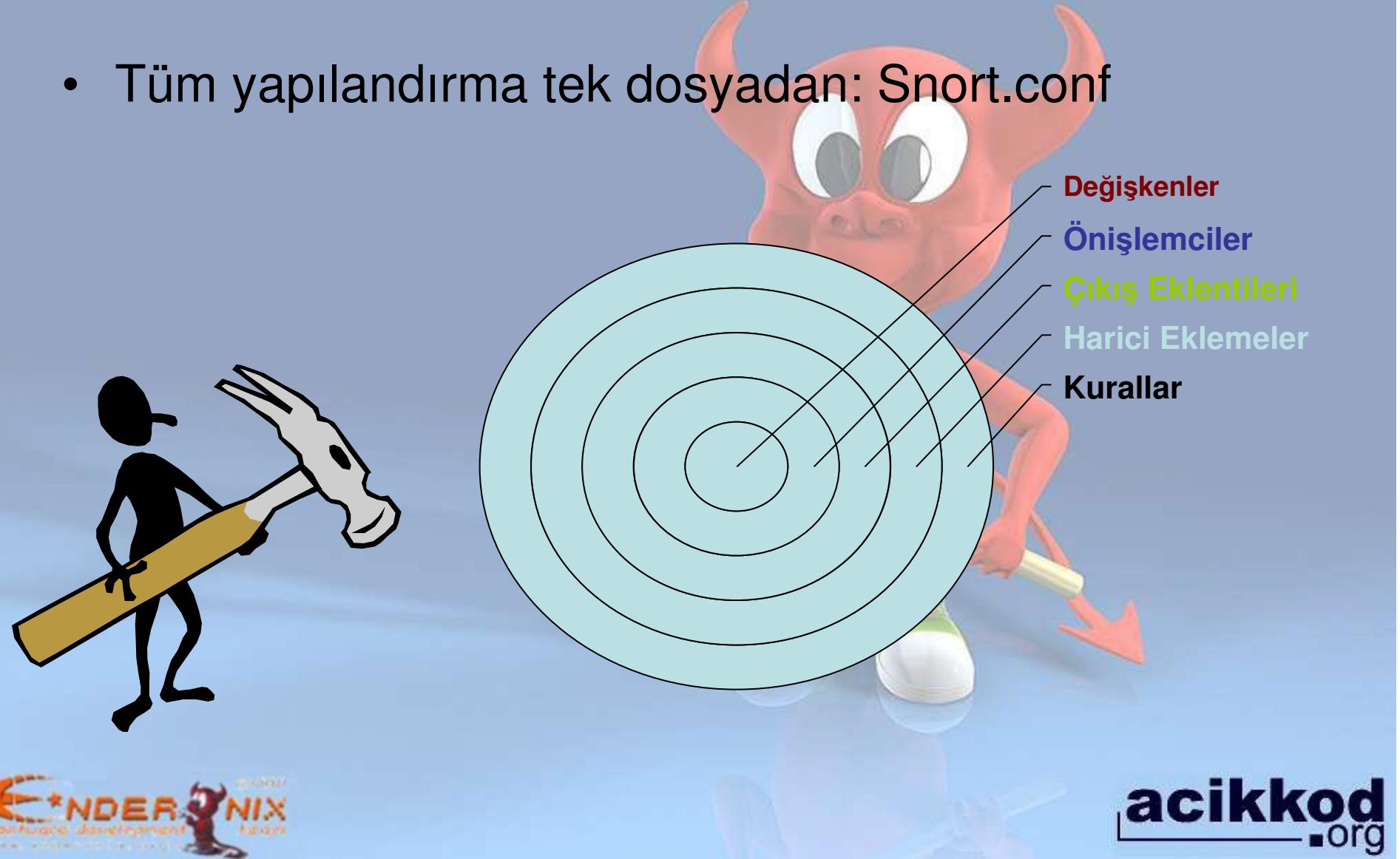


Snort Çalışma Modları -NIPS



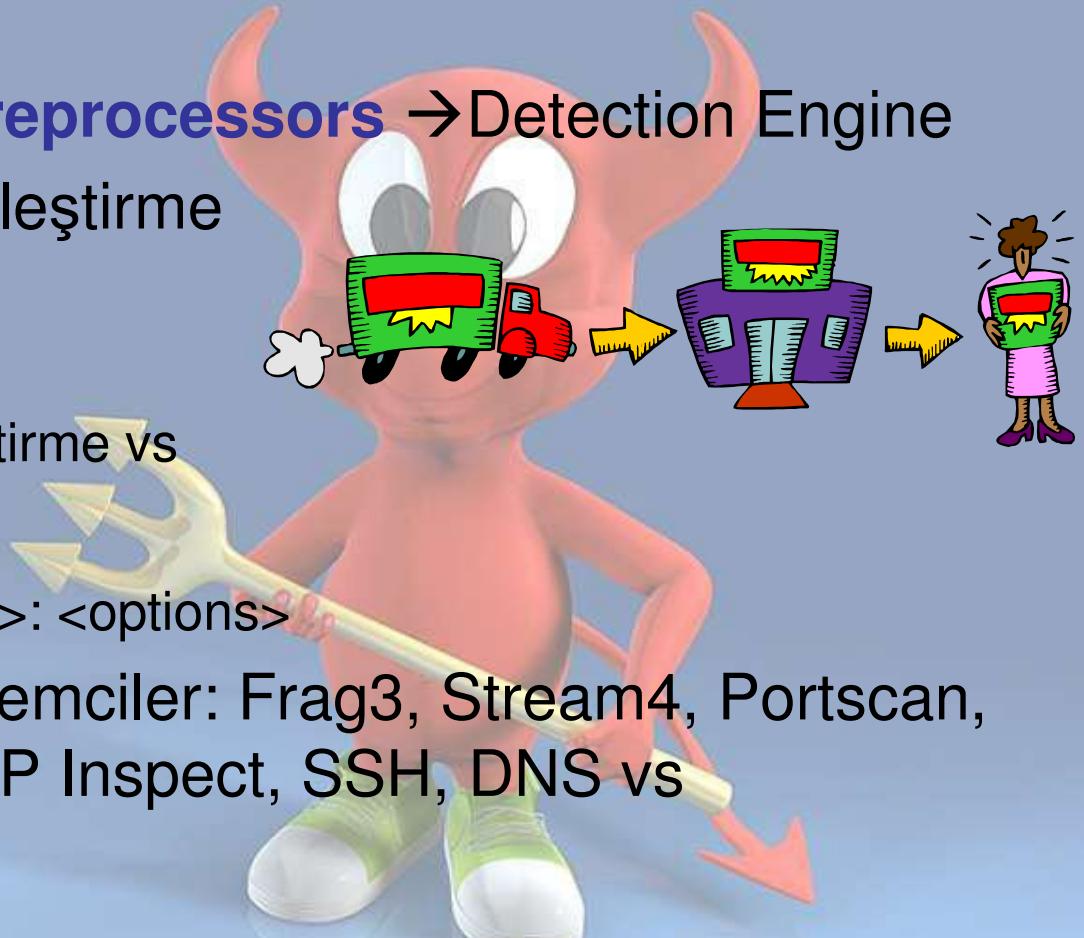
Temel Snort Yapılandırması

- Tüm yapılandırma tek dosyadan: Snort.conf



Ön İşlemciler (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 İşlemciler: Frag3, Stream4, Portscan, Telnet Decode, HTTP Inspect, SSH, DNS vs

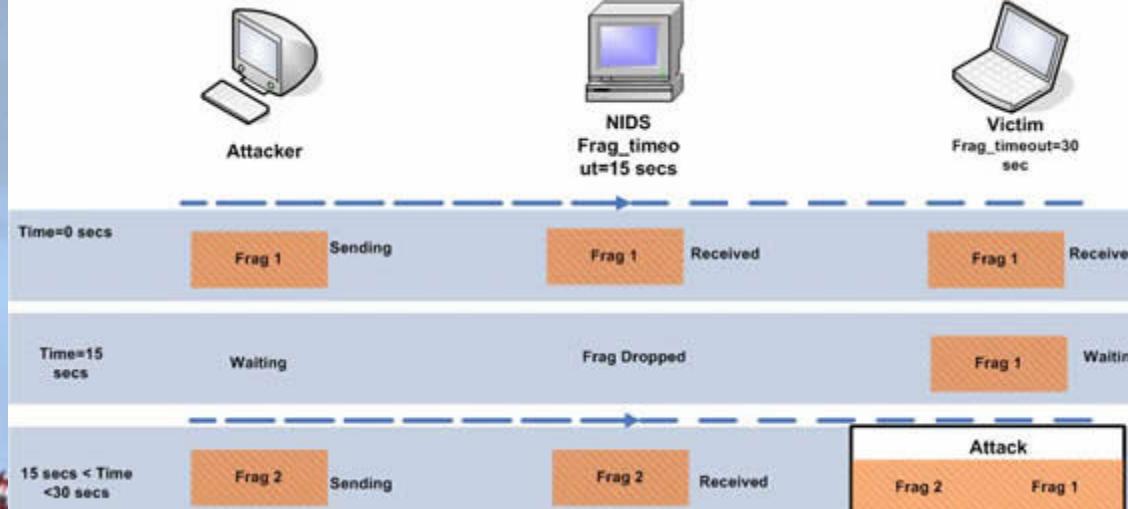


Stream4 &Frag3 Ön İşlemci

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

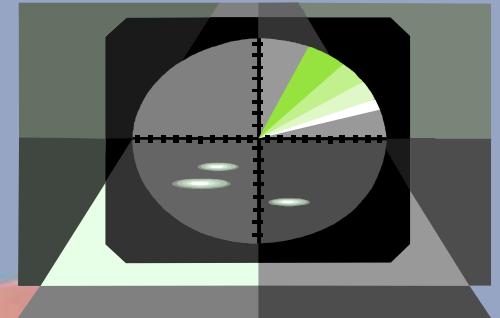


```
preprocessor frag3_global: prealloc_nodes 8192  
preprocessor frag3_engine: policy linux, bind_to 192.168.1.0/24  
preprocessor frag3_engine: policy first, bind_to [10.1.47.0/24,172.16.8.0/24]  
preprocessor frag3_engine: policy last, detect_anomalies
```



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

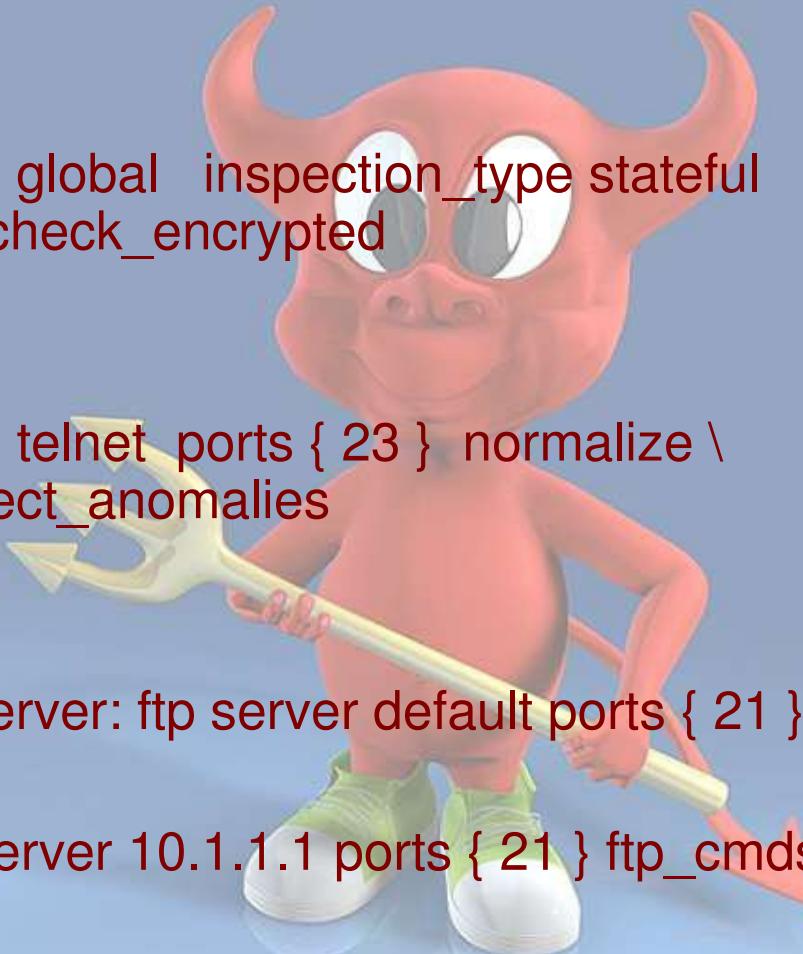
- Telnet protokolü için

- **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, gruplama kullanılabılır
- Analiz amaçlı Kullanım: Activate/Dynamic

```
activate tcp !$HOME_NET any -> $HOME_NET 143 (flags: PA; \
    content: "|E8C0FFFF|/bin"; activates: 1; \
    msg: "IMAP buffer overflow!");\n\ndynamic tcp !$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 ayrimı yapma
- **Offset:** içerik aramaya nerden başlanacağını belirtir.
- **Depth:** kaç bytelik alan aranacak

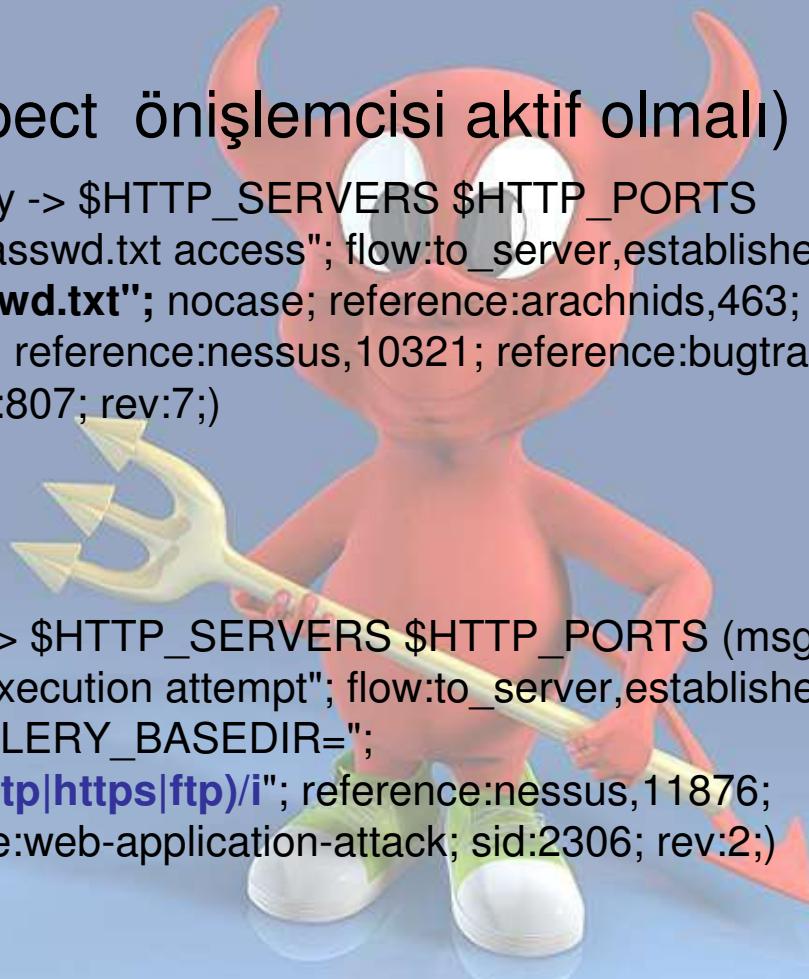
Kural Yazma -II

- 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;)
```

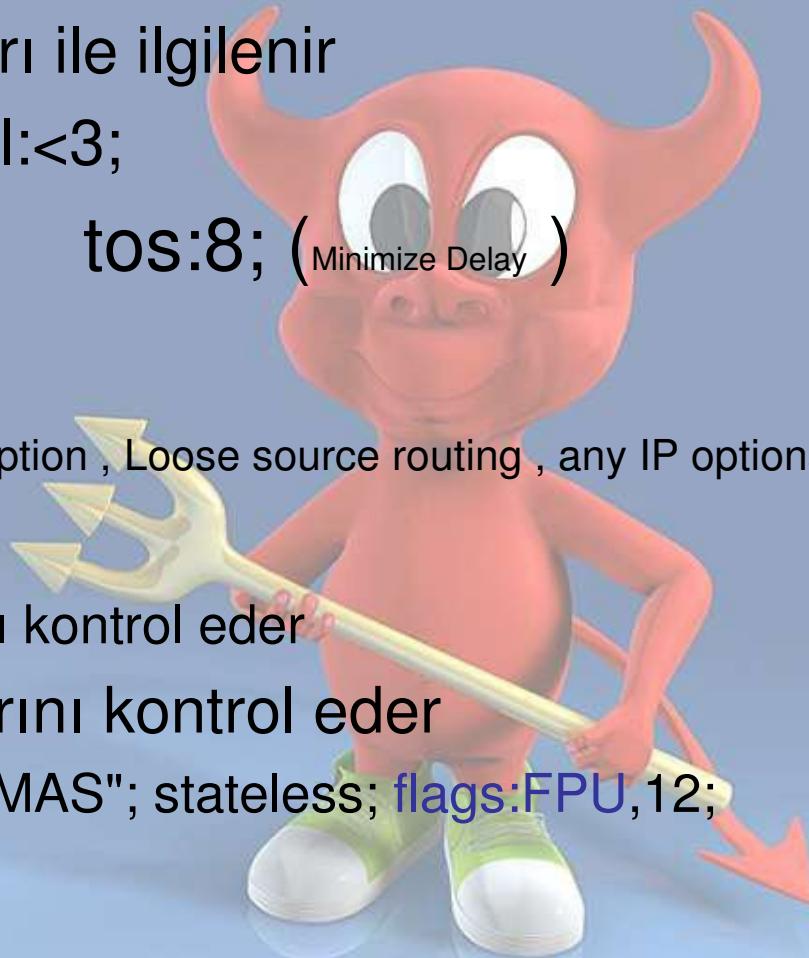
- PCRE Kullanımı

```
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 başlıklarını ile ilgilenir
- TTL Alanı kontrolü ttl:<3;
- IP Tos Alanı kontrolü tos:8; (Minimize Delay)
- Ipopts Alanı Kontrolü
 - 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;)

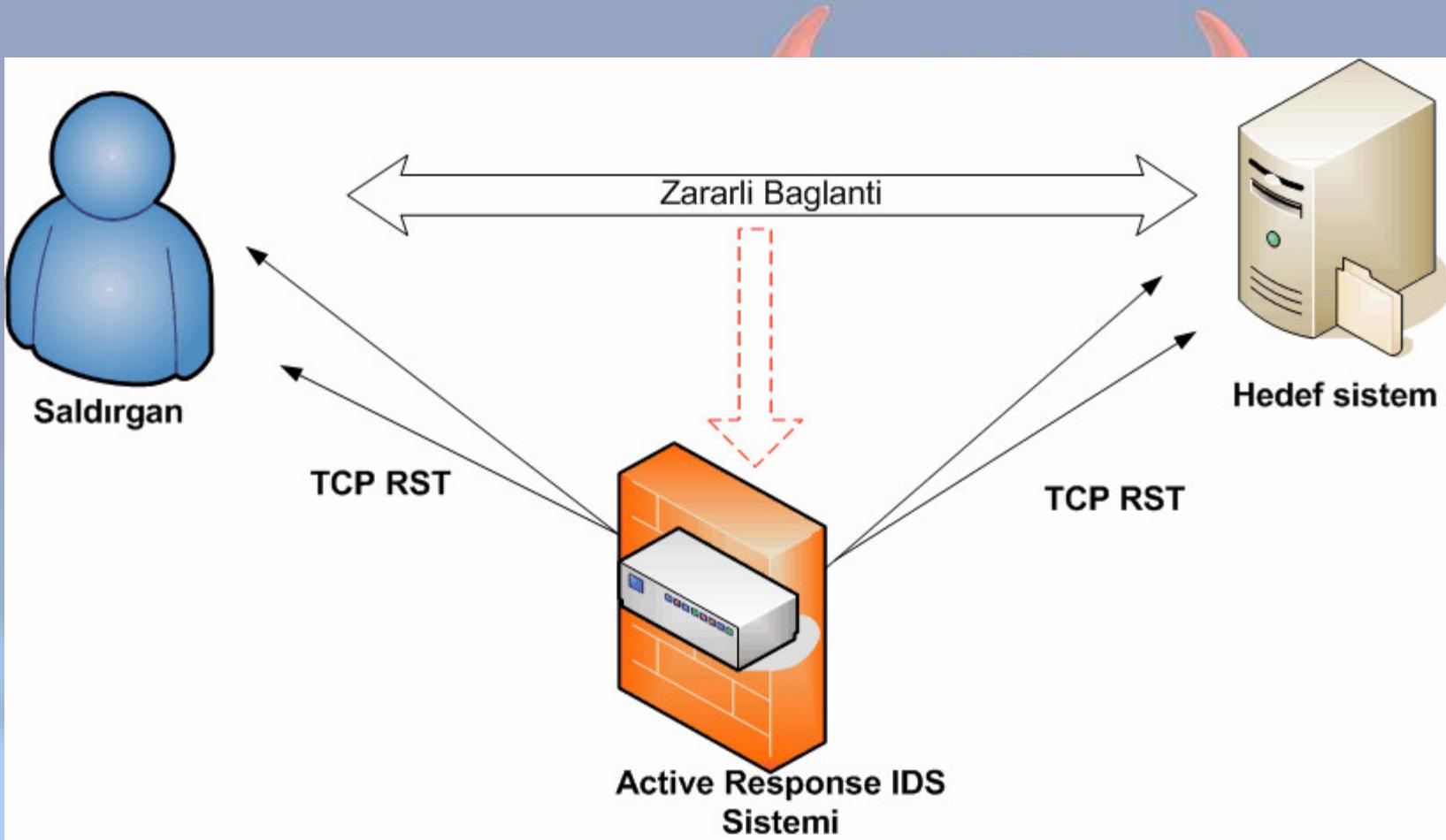
- icmp_id, ipopts, ack, window, rpc vs

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 browserine 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 Saldırıları Bloklama



Flexresp Kullanımı

- Kurulumda --enable-flexresp ile derlenmeli

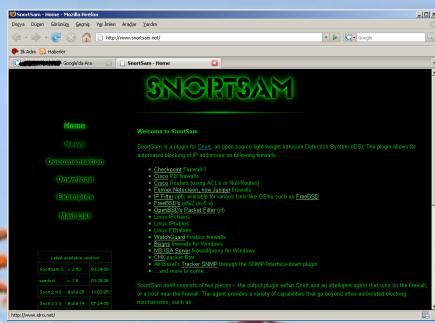
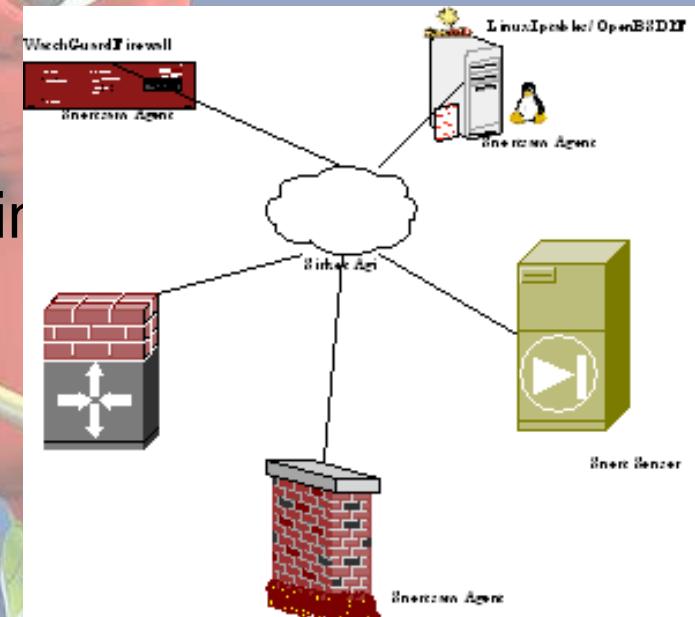
```
alert tcp $HOME_NET 2401 -> $EXTERNAL_NET any (msg:"MISC CVS invalid repository response"; flow:from_server,established; content:"error "; content:"\: no such repository"; content:"I HATE YOU"; classtype:misc-attack; sid:2009; rev:1;)
```

- 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 Engellemeye

- SnortSam -> Snort output plugin + Snortsam Agent
- Active Response Özelliği != IPS
- BeyazListe IP Desteği
- Ajan Snort arası şifreli iletişim
- Olaylar için loglama ve mail ile bildirme
- 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)



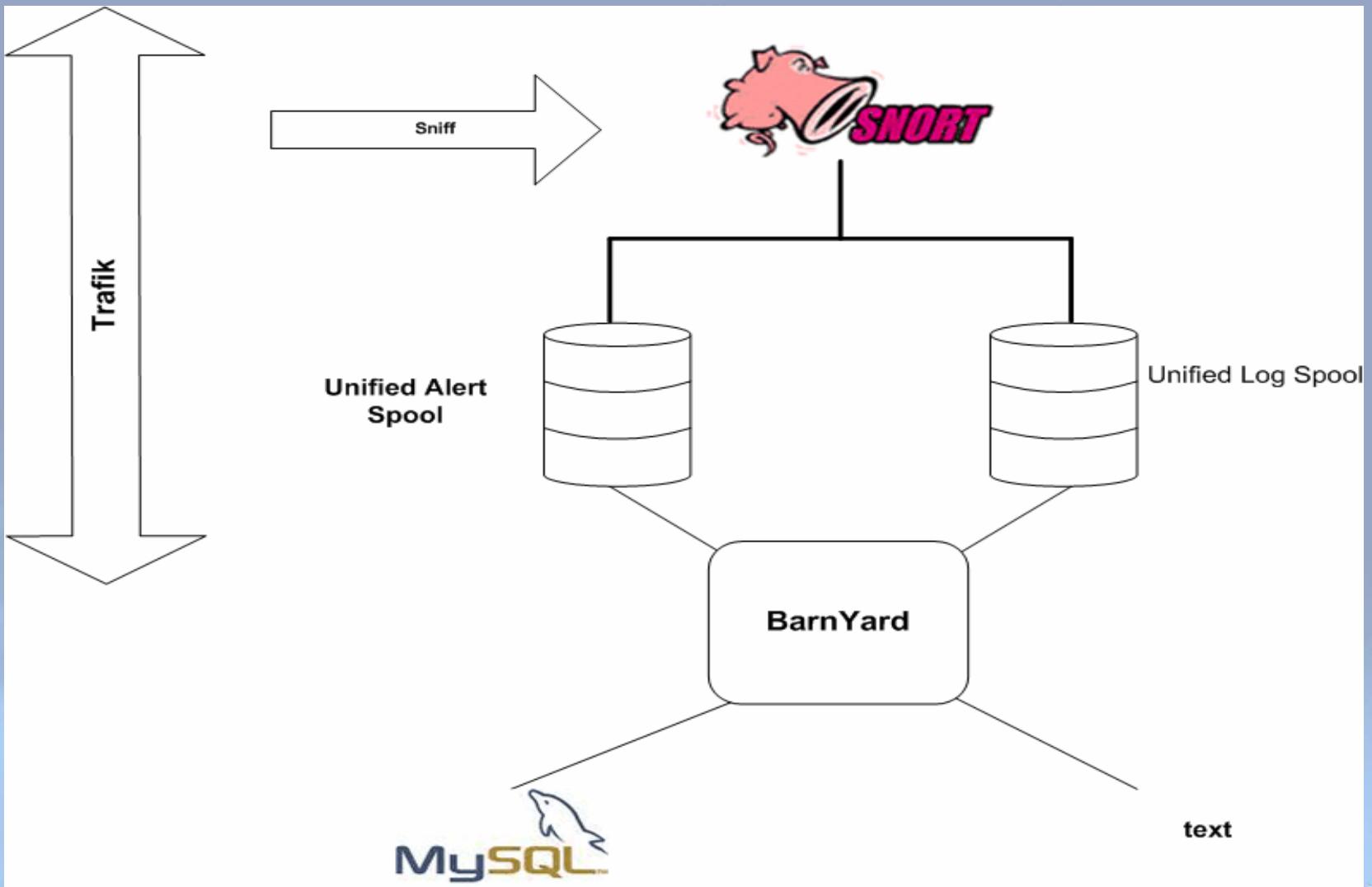
Düşük Performanslı IDS için

- 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 thresholdlarının düşürülmesi

Unified Output Eklentisi



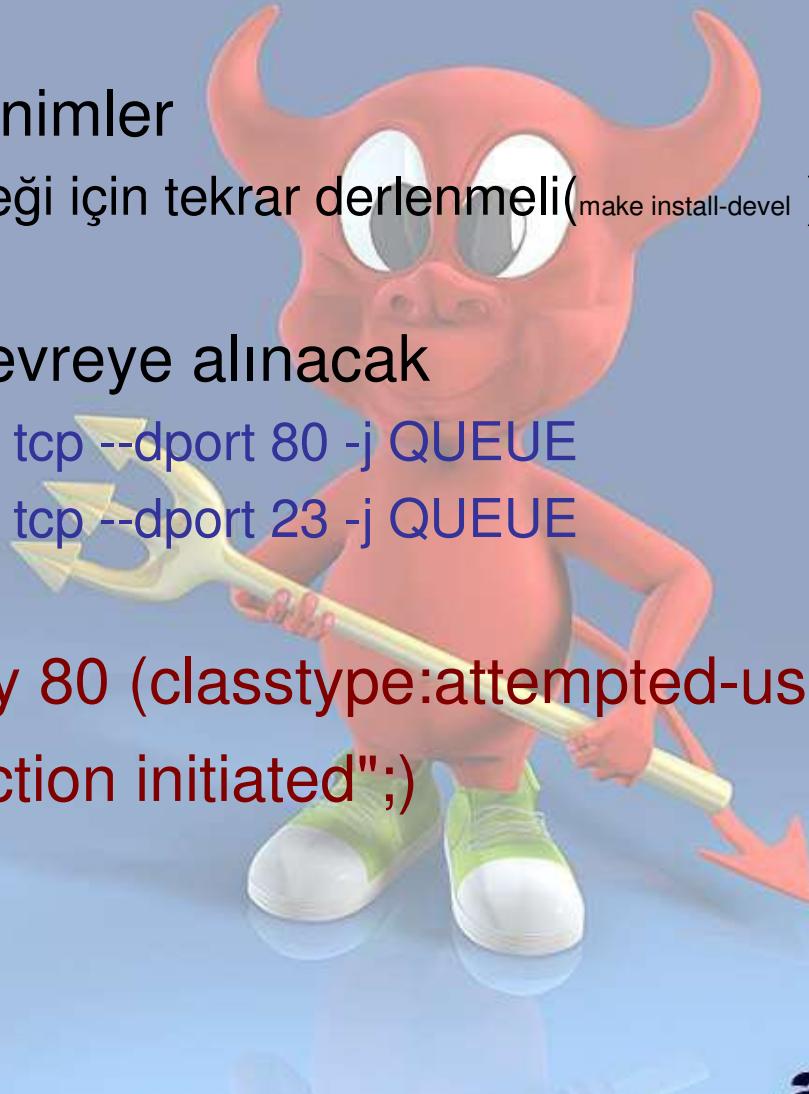
NIPS Olarak Snort

- 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, pishing vs amaçlı kullanım
- Linux -> Iptables, Libipq
- freeBSD -> IPFW, Divert Sockets
- OpenBSD -> PQ

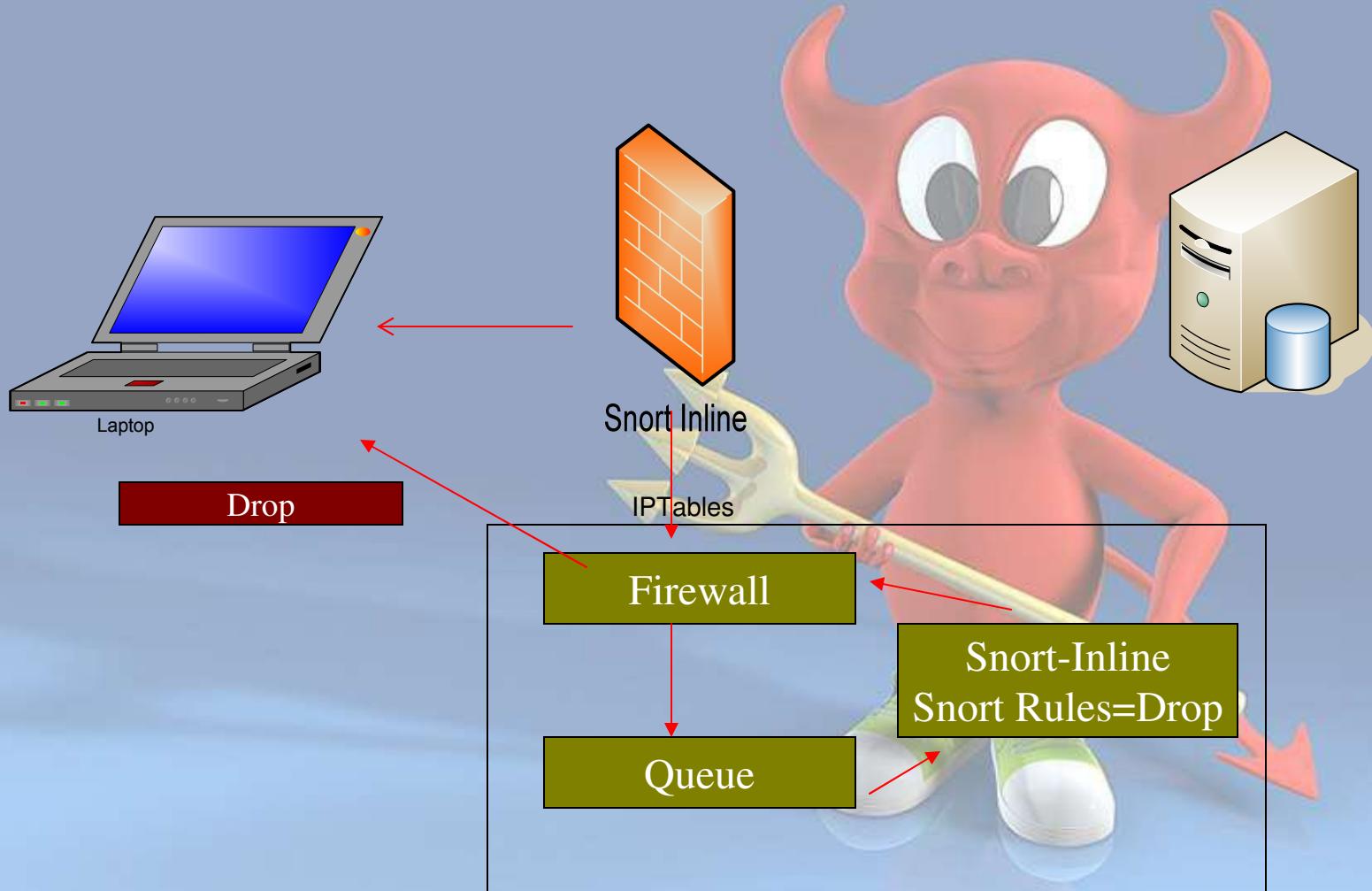
Snort_inline

- Kurulum için gereksinimler
 - Iptables, LibIpq 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

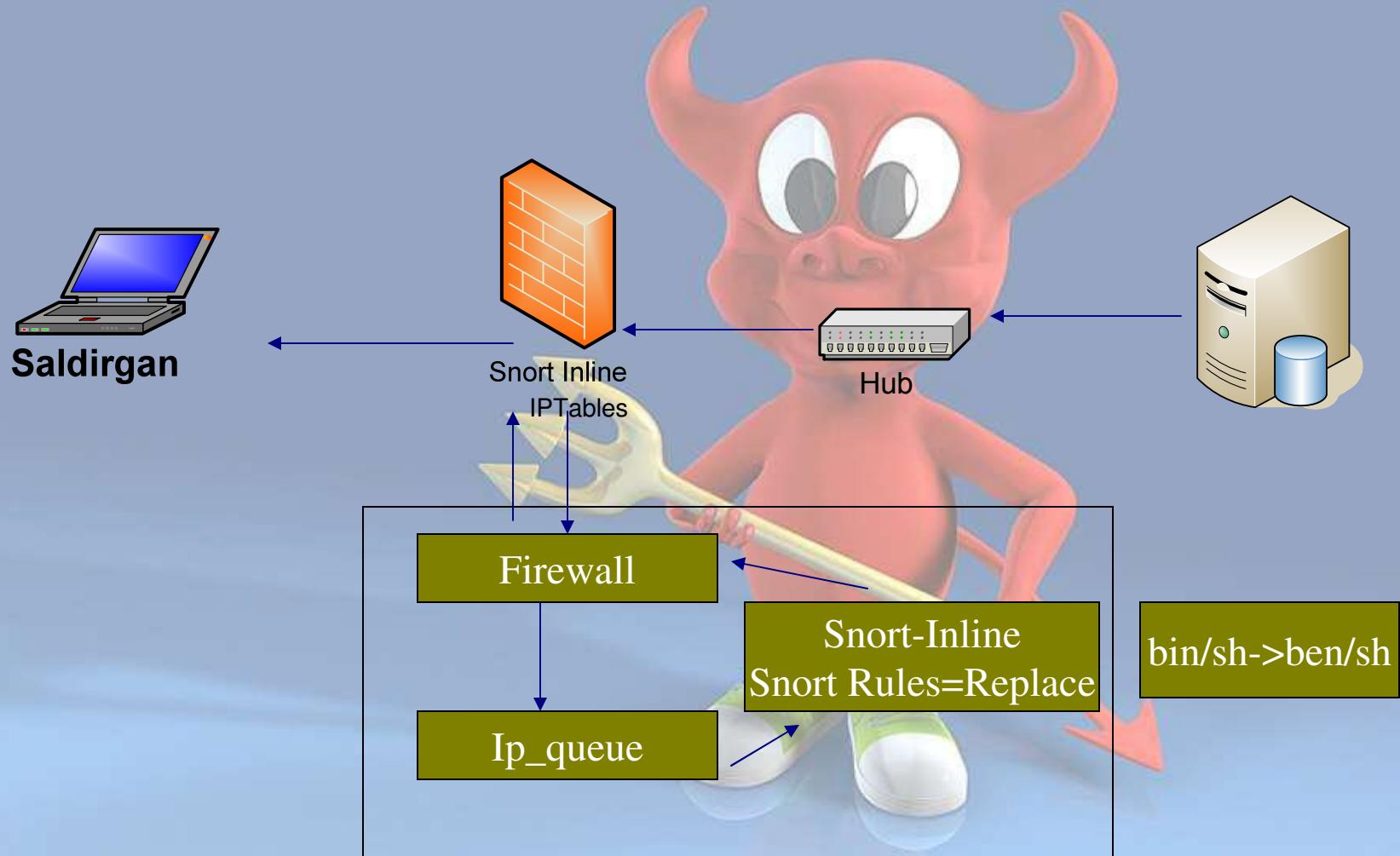
drop tcp any any -> any 80 (classtype:attempted-user;
msg:"Port 80 connection initiated";)



Snort-Inline Drop Mode



Snort-Inline Replace Mode



Yönetim Araçları

IDS Policy Manager

File Options Help

Policy Manager

Rule - WEB-MISC carbo.dll access

Name: WEB-MISC carbo.dll access Group: web-misc

Enabled: Signature ID: 1001 Revision: 7

Settings **Web References**

Action	Protocol	Classification	Priority
alert	tcp	attempted-recon	2

Source IP/Mask: \$EXTERNAL_NET Source Port: any Direction: > Destination IP/Mask: \$HTTP_SERVERS Destination Port: \$HTTP_PORTS

Rule Options:

```
flow:to_server,established;uricontent:"/carbo.dll";content:"icatcommand='";nocase;
```

References

Type	Value
bugtraq	2126
cve	1999-1069

Add Reference

OK Cancel

ENDER NIX
Software development
www.endernix.com.tr

actirroo.org

Log İzleme Araçları- BASE

Basic Analysis and Security Engine (BASE) - Mozilla

File Edit View Go Bookmarks Tools Window Help

Basic Analysis and Security Engine (BASE)

- Most recent Alerts: any protocol, TCP, UDP, ICMP
- Today's: alerts unique, listing; IP src / dst
- Last 24 Hours: alerts unique, listing; IP src / dst
- Last 72 Hours: alerts unique, listing; IP src / dst
- Most recent 15 Unique Alerts
- Last Source Ports: any , TCP , UDP
- Last Destination Ports: any , TCP , UDP
- Most frequent 5 Alerts
- Most Frequent Source Ports: any , TCP , UDP
- Most Frequent Destination Ports: any , TCP , UDP
- Most frequent 15 addresses: source, destination

Added 0 alert(s) to the Alert cache
Queried on : Thu October 14, 2004 22:02:36
Database: snort.log@localhost (schema version: 106)
Time window: [2004-09-02 16:05:49] - [2004-10-08 11:25:41]

Sensors: 1
Unique Alerts: 14
categories: 5
Total Number of Alerts: 84

- Src IP addrs: 5
- Dest. IP addrs: 9
- Unique IP links 13
- Source Ports: 68
 - TCP (68) UDP (0)
- Dest. Ports: 12
 - TCP (12) UDP (0)

Traffic Profile by Protocol

Protocol	Percentage
TCP	96%
UDP	0%
ICMP	4%
Portscan Traffic	0%

Search
Graph Alert data
Graph alert detection time

Alert Group Maintenance | Cache & Status | Administration

BASE 0.9.7.2 (by Kevin Johnson and the BASE Project Team
Built on ACID by Roman Danyliw)

Log İzleme Araçları- Aanval

Remote Assessment:: Aanval Console

http://demo.aanval.com/aanval/

Aanval Administrative Aanval Development RSS Feeds (90) Woohoo Standard

Remote Assessment: Aanval... Series 2 > Aanval Console™

Live Monitor Features Console Logout

Search > Got Help

Aanval Home > Main Console

Console Summary Frequent Events Frequent Offenders Community Chat

User Account Summary

User	root
User ID	102
Username	Demo User
Email	demo@aanval.com
Phone	888-569-2186
Organization	
City, State	Demo City, DM
Country	USA

Last Login 07/20/2006 02:52:53
Current IP 145.254.220.73

Edit User Profile

Miscellaneous

Console Time 07/20/2006 02:57:48

User Sensor Summary

Available Sensors	3
Currently Viewing	<input checked="" type="checkbox"/> Demo Sensor <input checked="" type="checkbox"/> Test Sensor 1 <input checked="" type="checkbox"/> Test Sensor 2

Update

Recent Search History

Date	Search
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17
07/20/2006	sip:217.160.227.17

User Graphs Summary

Total Events / Last 15 Days

07/06/2006	~300
07/07/2006	~400
07/08/2006	~450
07/09/2006	~600
07/10/2006	~550
07/11/2006	~500
07/12/2006	~300
07/13/2006	~400
07/14/2006	~600
07/15/2006	~450
07/16/2006	~400
07/17/2006	~350
07/18/2006	~2800
07/19/2006	~1000
07/20/2006	~100

Select Additional Charts and Graphs

Console Log Summary

ID	User ID	IP	Module	Action	Miscellaneous	Date / Time
25224	102	71.113.17.204	prv_main	Private Ops Navigation		07/20/2006 01:57:48
25223	102	71.113.17.204	prv_mainDisplayPost	Private Ops Navigation		07/20/2006 01:57:45
25222	102	71.113.17.204	prv_main	Private Ops Navigation		07/20/2006 01:57:27
25221	102	71.113.17.204	prv_mainDisplayPost	Private Ops Navigation		07/20/2006 01:57:25
25220	102	71.113.17.204	prv_main	Private Ops Navigation		07/20/2006 01:55:39

Aanval 2.2 (Abram) - Build: 20210 | Copyright 2004-2006 Released Under the Remote Assessment Commercial Use License (C1-RA1008)
Server response time: 0.31 - Stamp: 1153389468.02.01 - Get: 105 - Set: 3 - M: 866.33 KB in 90
StatCache used 1 cached data results for performance - Reload page without StatCache

United States United Kingdom Germany France Spain Italy

IDS/IPS atlatma araçları ve korunma yöntemleri

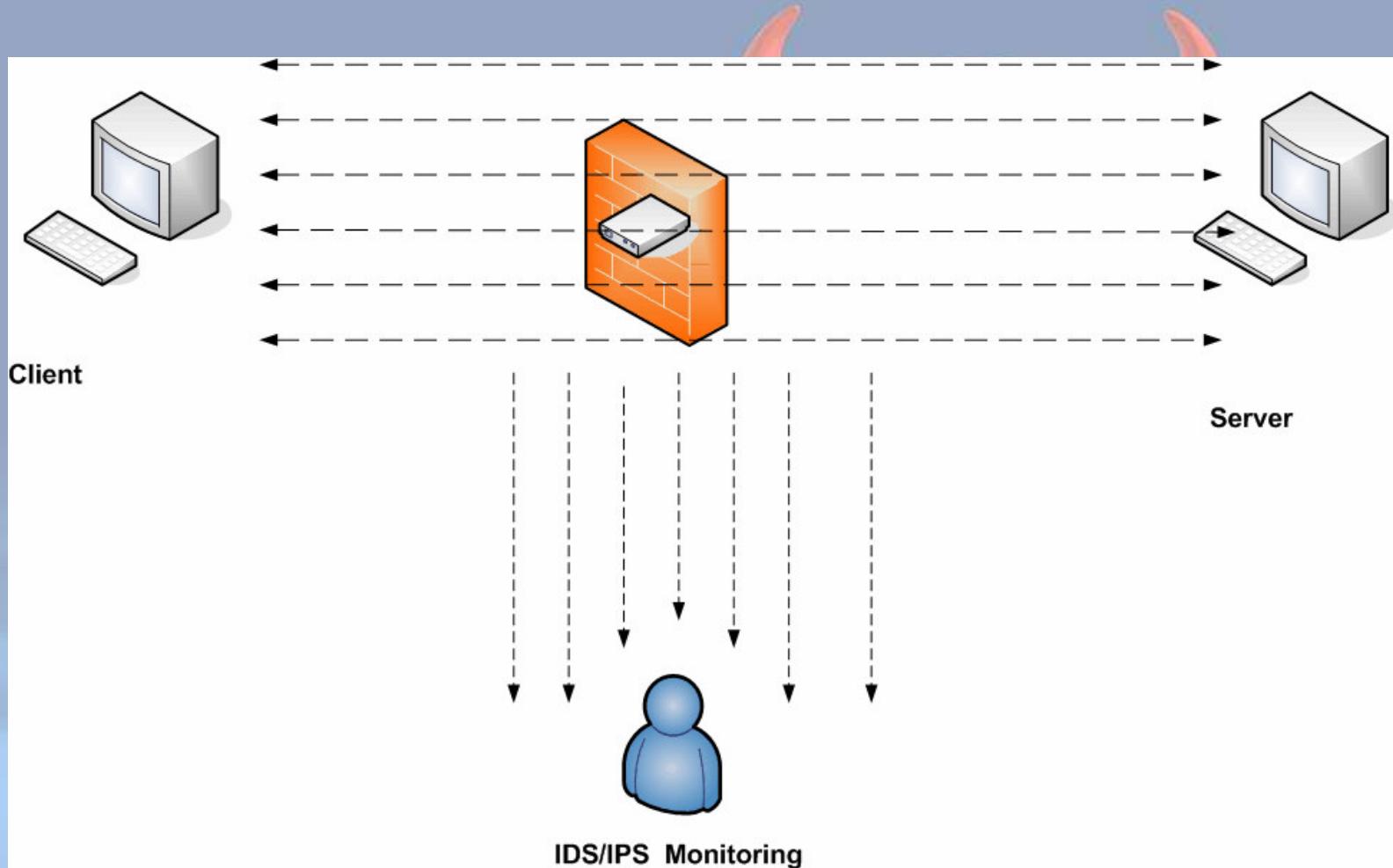
	Snort			ISS RealSecure		
Exploit	Baseline Attack	Mutated Attack	Evasion Technique	Baseline Attack	Mutated Attack	Evasion Technique
WUFTP	Detected	Evaded	Telnet ctrl seq Shellcode <u>IP splitting</u>	Detected	Evaded	Telnet ctrl seq Shellcode
WUIMAP	Detected	Evaded	Zero prefix Shellcode	Detected	Evaded	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 <u>IP splitting</u>	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 yetenegi

```
ids-conn=192.168.0.10:23:10.1.7.1:1025:PA:TCP:0: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 guvenligi ipucları
 - TCP/IP Guvenligi
- Olympos Security(www.olympos.org)
- www.EnderUNIX.org
- <http://netsec.huzeyfe.net> – Netsec Listesi



Sorularınız



Teşekkürler **acikkod.org**