

BİLGİ GÜVENLİĞİ AKADEMİSİ

www.bga.com.tr

DoS / DDoS Saldırıları ve Korunma Yolları Eğitimi

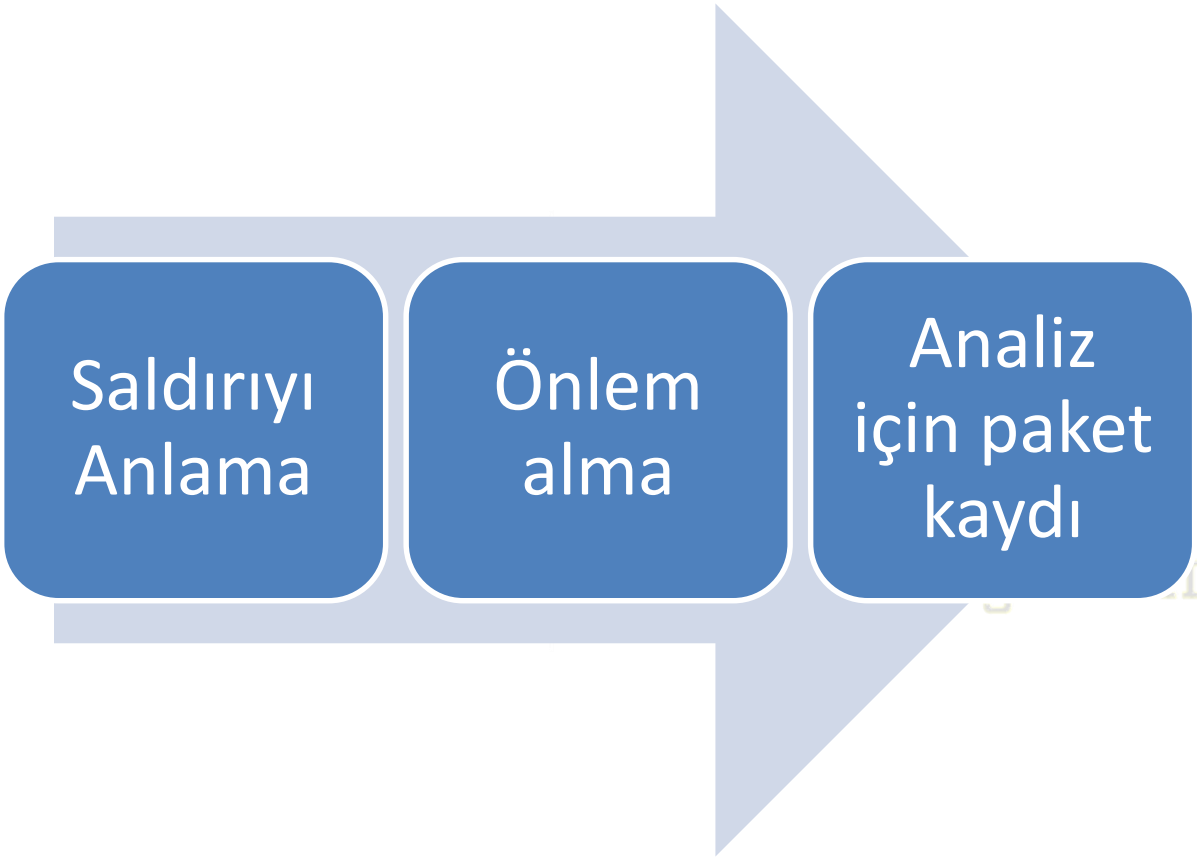
@2012

Örnek Eğitim Notu

bilgi@bga.com.tr



Saldırı Çeşitleri ve Korunma Yolları



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

BİLGİ GÜVENLİĞİ AKADEMİSİ www.bga.com.tr

DDOS Saldırı Analizi

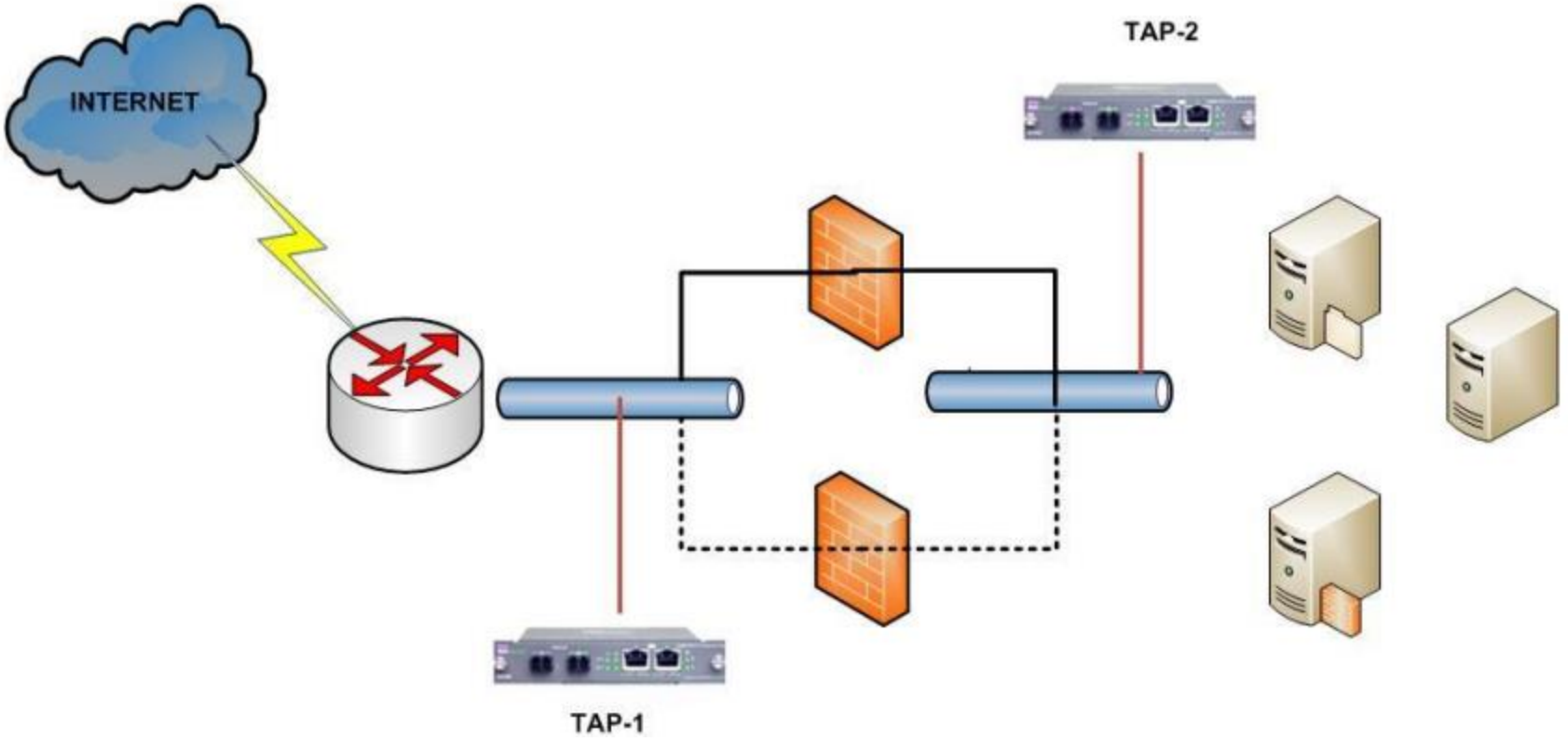
- DDoS saldırılarında dikkat edilmesi gereken iki temel husus vardır.
  - İlki saldırıyı engelleme
  - İkincisi saldırının kim tarafından ne şiddette ve hangi yöntemler, araçlar kullanılarak yapıldığınının belirlenmesidir.
- Analiz kısmı genellikle unutulur fakat en az engelleme kadar önemlidir.
  - Aynı saldırı tekrar ederse nasıl engelleme yapılacağı konusunda yol haritası çıkarılmış olmalıdır.

Bilgi Güvenliği BGA AKADEMİSİ www.bga.com.tr

DDoS Analizi İçin Gerekli Yapının Kurulması

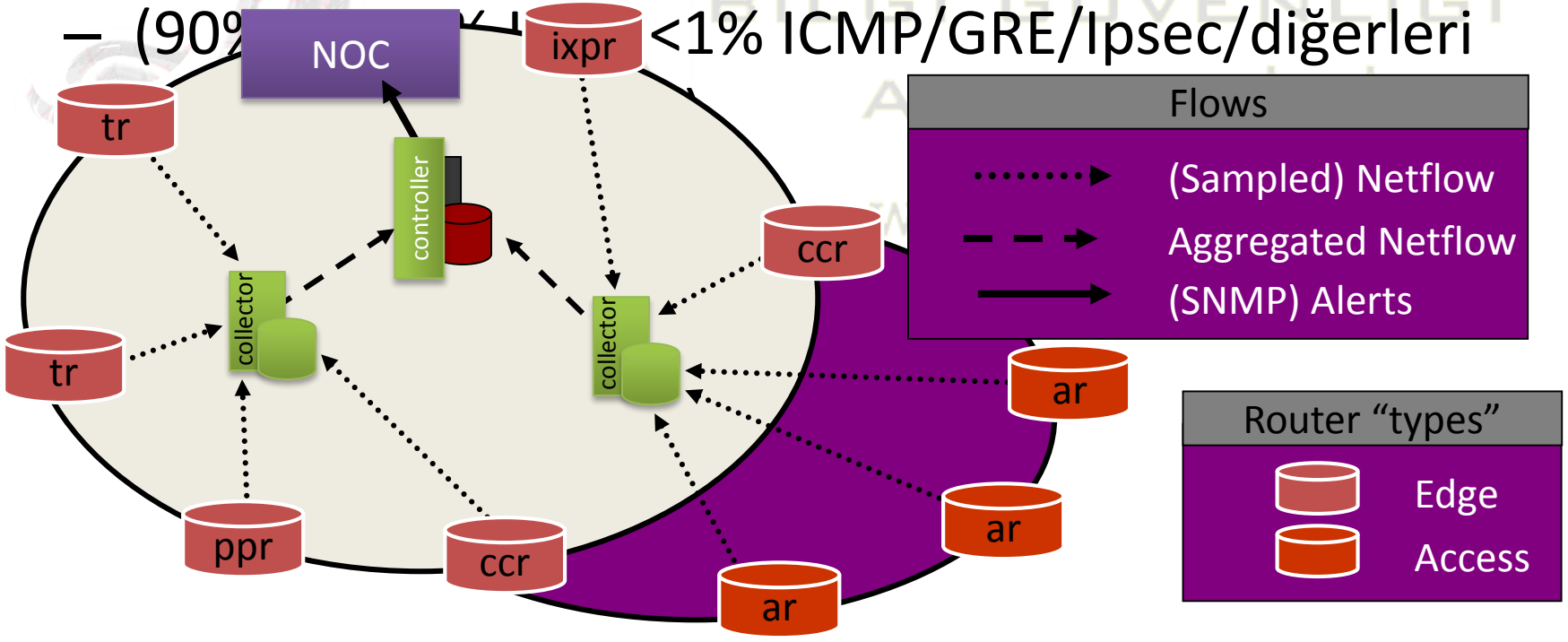
- Amaç DDoS saldırılarında otomatik olarak devreye girip saldırıya ait delil olabilecek paketlerin kaydedilmesi.
- Saldırı anında paketler kaydedilirse saldırıya ait tüm detaylar istenildiği zaman öğrenilebilir.
- Paket kaydı hedef sistem üzerinde (Windows/Linux) veya ağ ortamında TAP/SPAN portu aracılığıyla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

DDoS Analizi İçin Gerekli Yapının Kurulması



Distributed Denial of Service

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



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 IPadresleri mi kullanılmış?
- DDoS saldırısı hangi ülke/ülkelerden geliyor?

BİLGİ GÜVENLİĞİ BGA AKADEMİSİ www.bga.com.tr

Saldırı Analizinde Kullanılan Araçlar

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

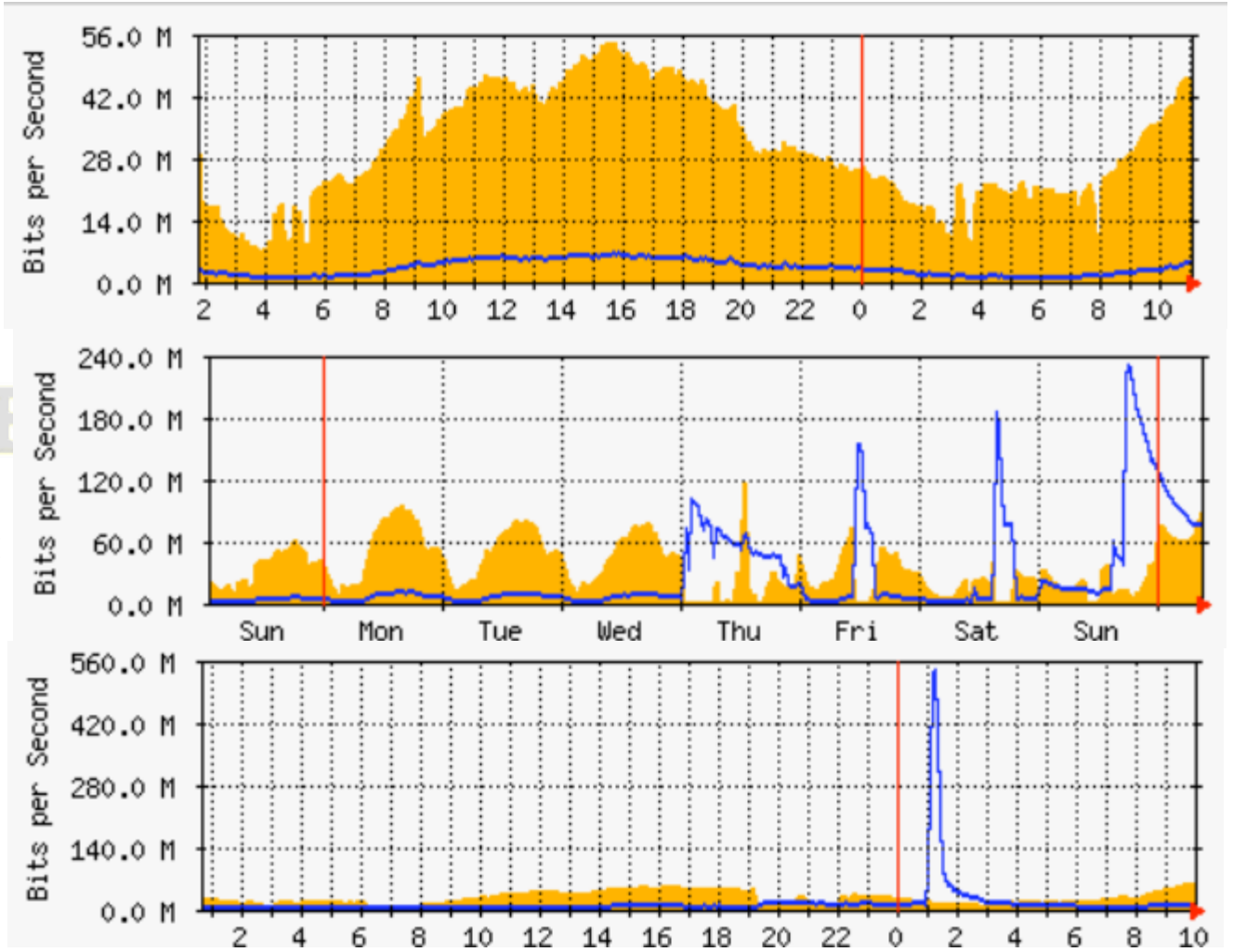
BİLGİ GÜVENLİĞİ
BGA
AKADEMİSİ
www.bga.com.tr

MRTG/RRD Grafikleri

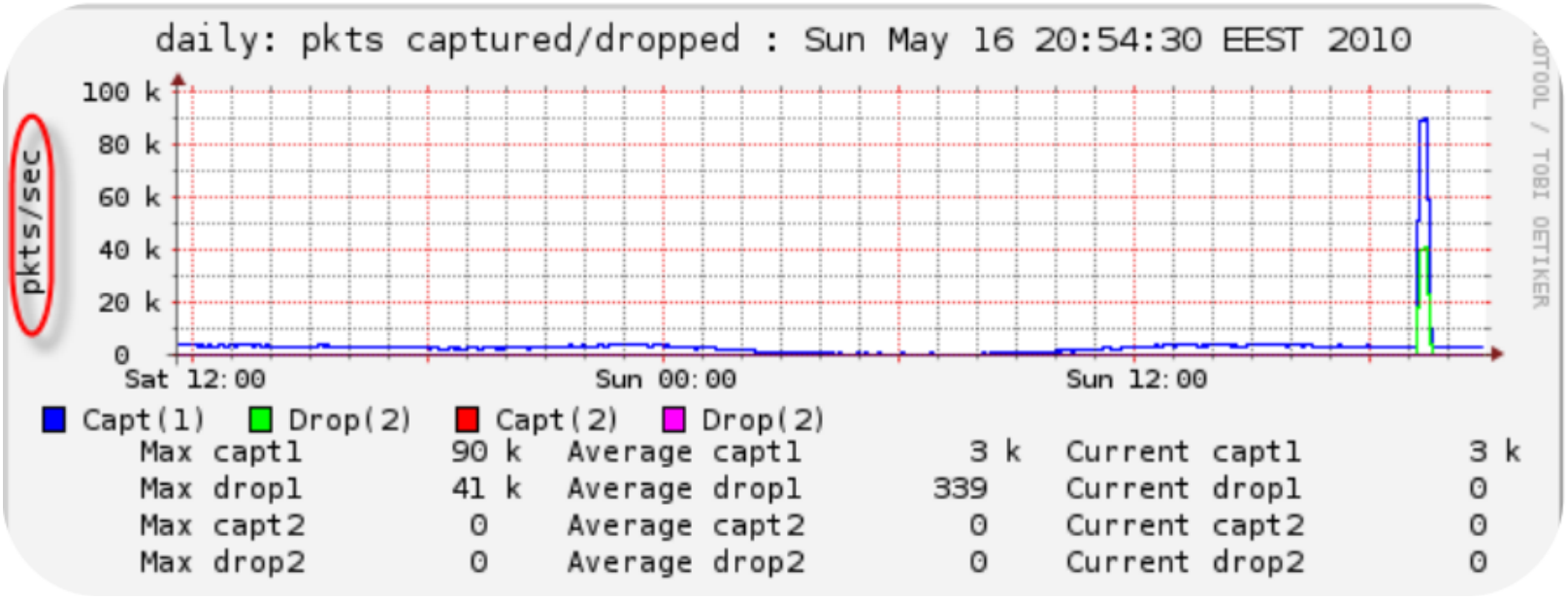
Normal Trafik

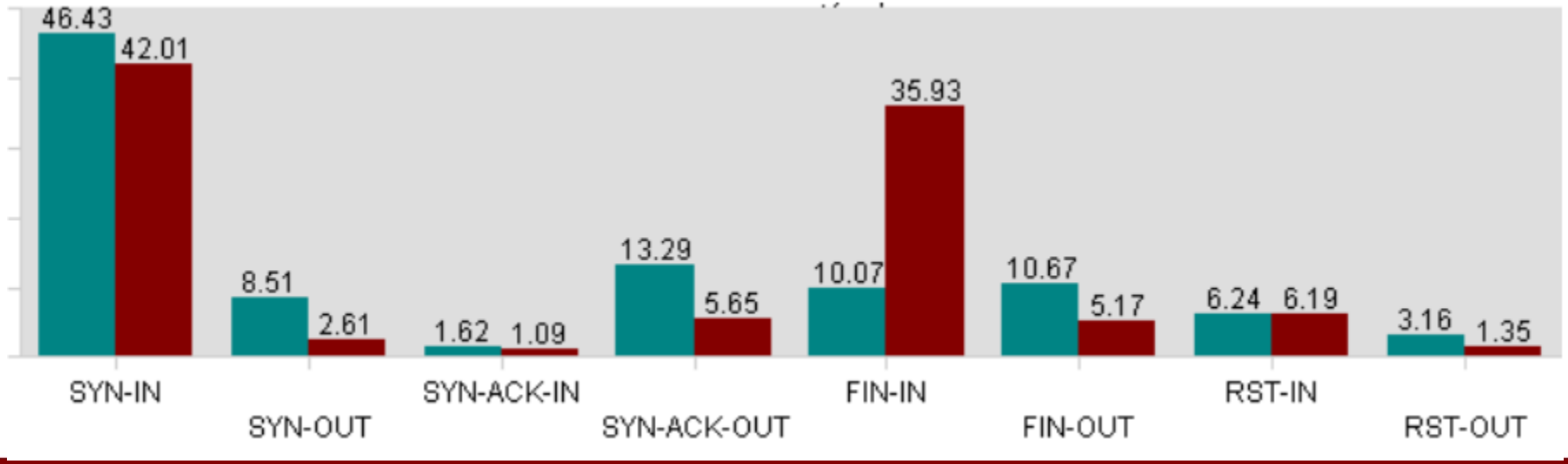
DDOS 1. Gün

DDOS 2.Gün



İstatistiksel Analiz





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.

BGA BİLGİ GÜVENLİĞİ AKADEMİSİ www.bga.com.tr

Tcpdump ile DDoS Paketlerini 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

BILGI GÜVENLİĞİ
BGA AKADEMİSİ
www.bga.com.tr

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**

BİLGİ GÜVENLİĞİ AKADEMİSİ
www.bga.com.tr

Tcpdstat İle DDoS tipini Belirleme

```
# 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 -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

BİLGİ GÜVENLİĞİ
BGA AKADEMİSİ
www.bga.com.tr

SYN Flood Saldırısı Analizi

- **# 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

BİLGİ GÜVENLİĞİ BGA AKADEMİSİ www.bga.com.tr

ACK Flood Analizi

- Tcpdump kullanarak ACK bayraklı paketleri ayıklama
- # tcpdump -i bce1 -n ‘tcp[13] & 16 != 0’

BGA BİLGİ GÜVENLİĞİ AKADEMİSİ www.bga.com.tr

FIN Flood Analizi

- Tcpdump kullanarak FIN bayraklı paketleri ayıklama
- # tcpdump -i bce1 -n ‘tcp[13] & 1 != 0’ and tcp port 80

BİLGİ GÜVENLİĞİ
BGA
AKADEMİSİ
www.bga.com.tr

HTTP GET Flood Saldırısı

- 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.

BİLGİ GÜVENLİĞİ BGA AKADEMİSİ www.bga.com.tr

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.

BİLGİ GÜVENLİĞİ AKADEMİSİ
BGA
www.bga.com.tr

Tcpstat

```
[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

- 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.

Spoof IP Belirleme

- 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-II

- Tek cümleyle özetleyecek olursak:

Eğer aynı IPden birden fazla bağlantı yoksa spoofed IP kullanılmış olma ihtimali yüksektir.

```
#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

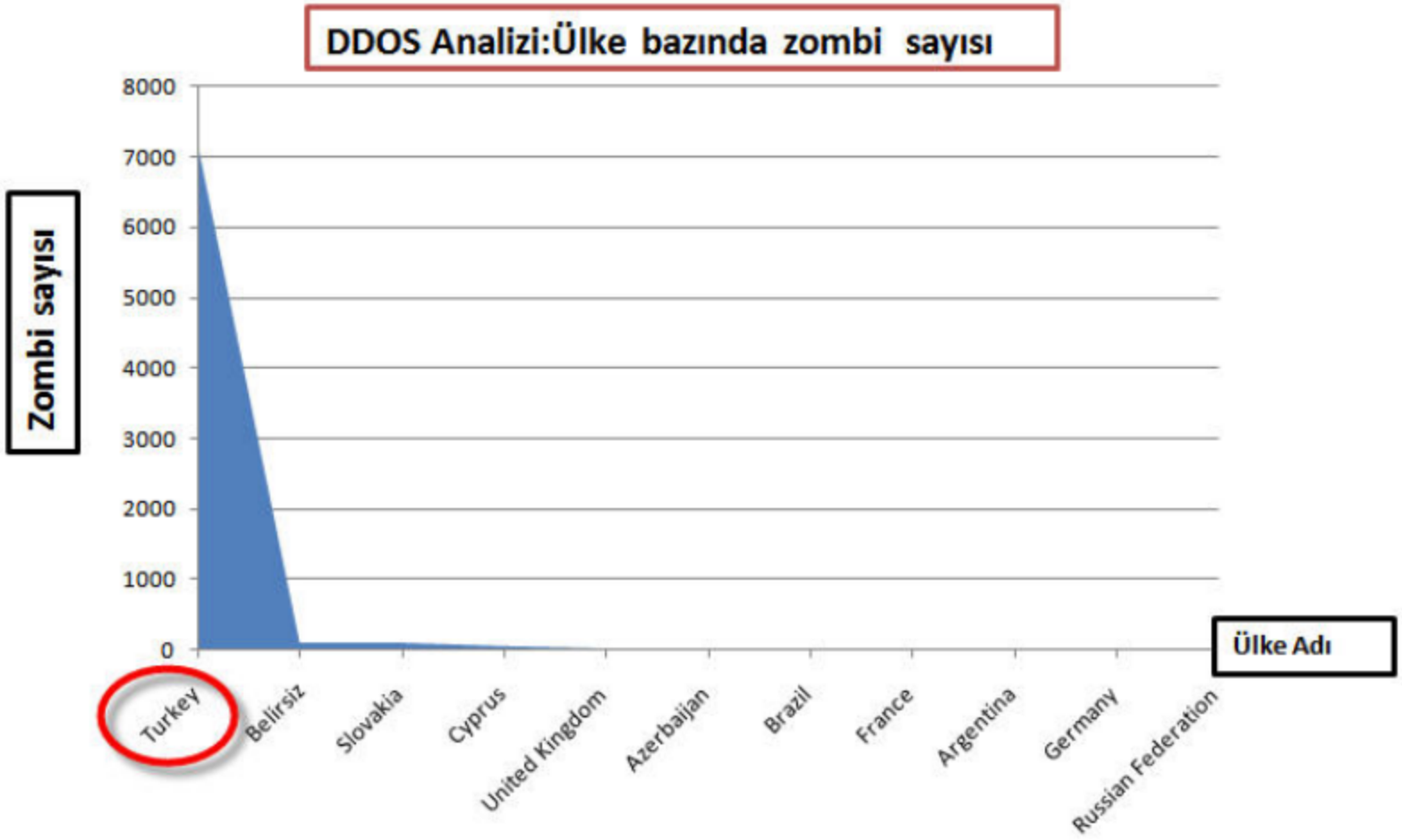
- HTTP GET flood saldırılarında IP spoofing yapmak mümkün değildir.
- Bir sistemin HTTP isteği gönderebilmesi için öncelikli olarak 3lü el sıkışmasını tamamlaması gerekmektedir.
- Günümüz işletim sistemi/ağ/güvenlik cihazlarında 3'lü el sıkışma esnasında TCP protokolünü kandırarak IP spoofing yapmak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

BİLGİ GÜVENLİĞİ BGA AKADEMİSİ www.bga.com.tr

HTTP Flood Yapan IP Adresleri

```
# 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
```

Saldırıda Kullanılan IP Adresleri Hangi Ülkeden?



Ülke Bulma Scripti

```
[root@depdep huzeyfe]# 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)
```

Netstat İle Linux Sistemlerde Analiz

```
netstat -atn |grep :80 |grep -v 8080| awk '{print $5}'|awk -F: '{print $1}'|sort -n |uniq -c|awk '{if ($1 > 10) {print }}'
```

```
root@server [~]# netstat -atn |grep :80 |grep -v 8080| awk '
int }}'
     16 72.32.9.30
     11 78.163.143.2
     12 78.163.203.195
     11 78.165.192.145
     14 78.168.47.177
     37 78.172.184.167
     11 78.173.90.112
     11 78.187.238.108
     13 78.189.21.241
     11 85.101.9.127
     12 88.226.180.44
     21 88.226.2.134
     13 88.226.72.202
     11 88.229.122.213
     16 88.230.202.101
     12 88.244.42.163
     15 88.245.225.175
     19 94.54.116.35
     39 127.0.0.1
     25 212.65.132.11
```

Wireshark Kullanarak DDoS Analizi

- Display filter özelliği kullanılır
- Bir pakete ait tüm başlık bilgileri ve payload seçilerek inceleme yapılabilir
  - User-Agent:Boş olan HTTP GET istekleri gibi

BİLGİ GÜVENLİĞİ
BGA AKADEMİSİ
www.bga.com.tr

BGA İletişim



www.bga.com.tr

blog.bga.com.tr



twitter.com/bgasecurity

facebook.com/BGAkademisi



bilgi@bga.com.tr

egitim@bga.com.tr