DOS, DDOS Atakları ve Korunma Yöntemleri

Huzeyfe ÖNAL
huzeyfe@lifeoverip.net
http://www.lifeoverip.net

Ben kimim?

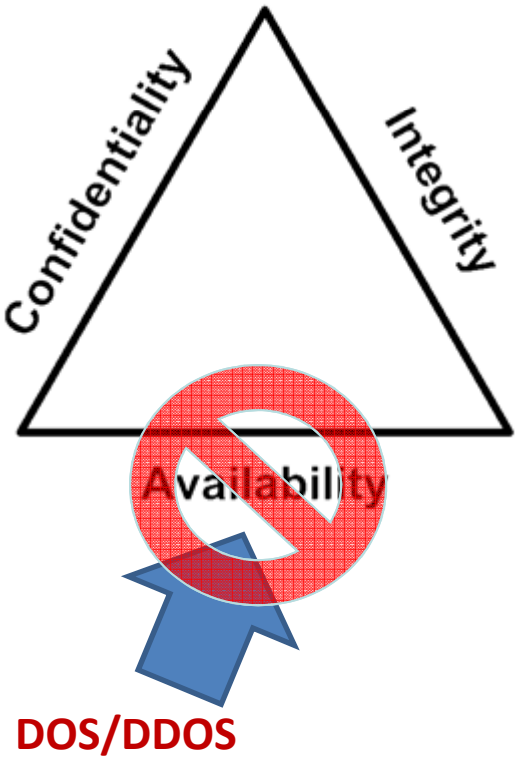
- Kıdemli Ağ Güvenliği Araştırmacısı
- Pentester
- Güvenlik Eğitmeni
  - http://www.guvenlikegitimleri.com
- Blog yazarı
  - http://blog.lifeoverip.net
- Kıdemli DOS/DDOS Uzmanı ☺

Ajanda

- Genel Kavramlar
- DOS saldırılarında Neden, nasıl, amaç, kim soruları ve cevapları
- DOS/DDOSDDOS Çeşitleri
  - Protokollere göre DOS/DDOS çeşitleri
- Korunma Yöntemleri
- 75 dakika sunum % 45 dakika soru cevap / demo
  - Uzuun bir konu(15 saatlik eğitim)
  - Sık kullanılan DOS yöntemlerini ele alacağım

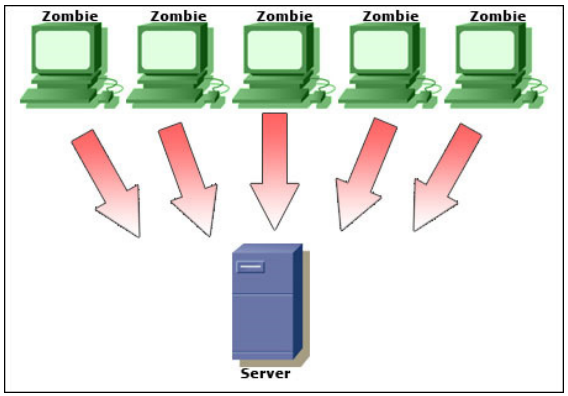
Genel Kavramlar

- DOS(Denial Of Service)
- DDOS(Distributed Denial Of Service)
- Zombi
- BotNet(Robot Networks)
- IP Spoofing
- FastFlux networks



DOS ? DDOS

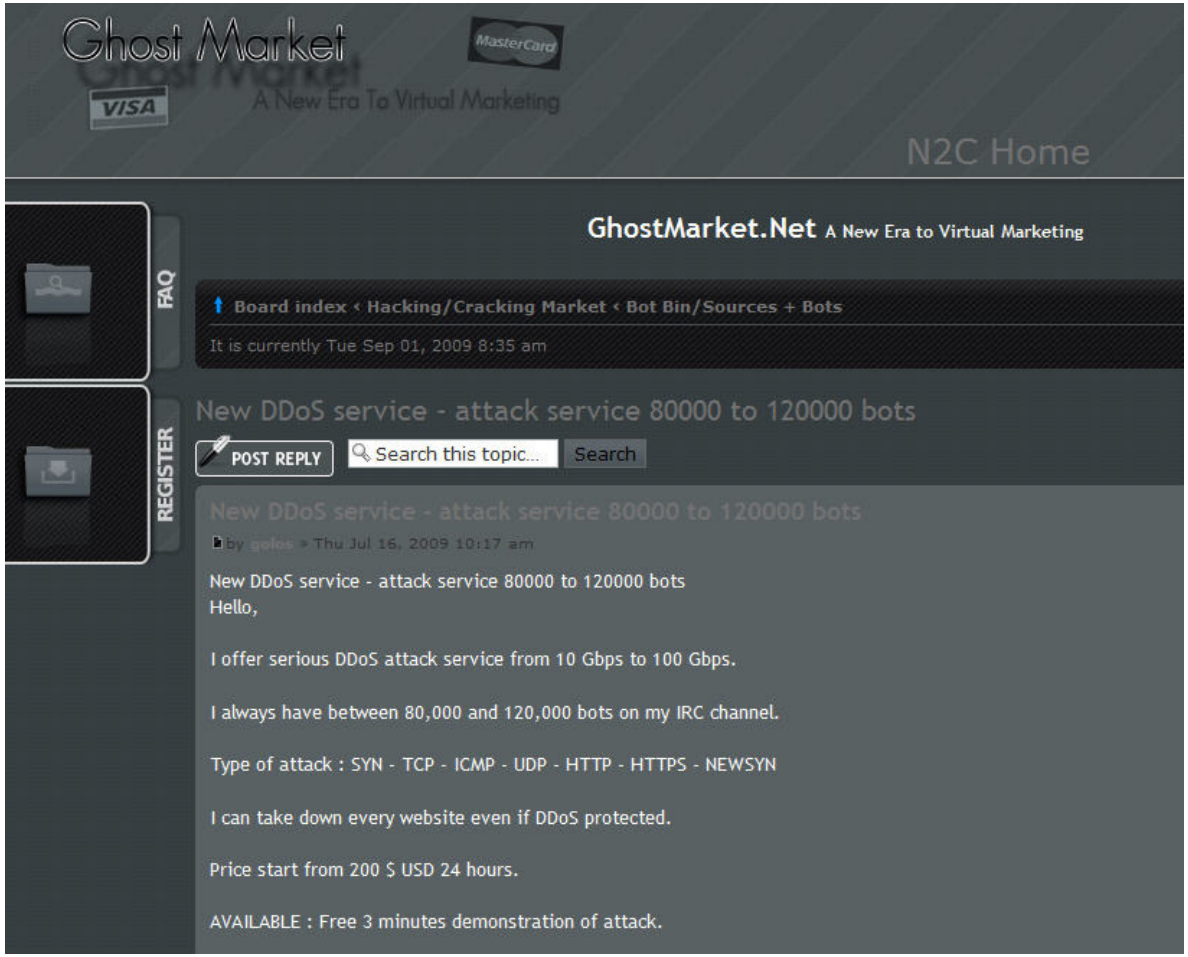
- DOS(Denial Of Service) = sistemleri çalışamaz hale getirmek için yapılan saldırı tipi
- DDOS(Distrubuted Denial of Service) DOS saldırısının yüzlerce, binlerce farklı sistemden yapılması
- Genellikle spoof edilmiş ip adresleri ve zombiler kullanılır



Zombi & Botnet

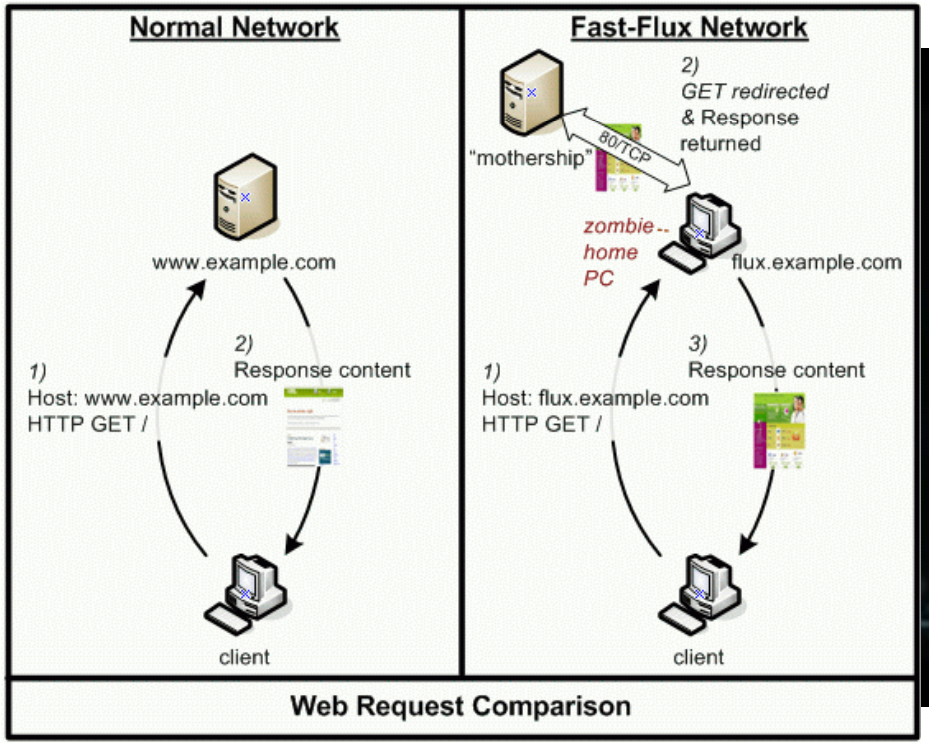
- Zombi: Emir kulu
  - Çeşitli açıklıklardan faydalanılarak sistemlerine sızılmış ve arka kapı yerleştirilmiş sistemler
  - Temel sebebi: Windows yamalarının eksikliği
- BotNet – roBOTNETworks
- Zombilerden oluşan sanal yıkım orduları
- Internette satışı yapılmakta

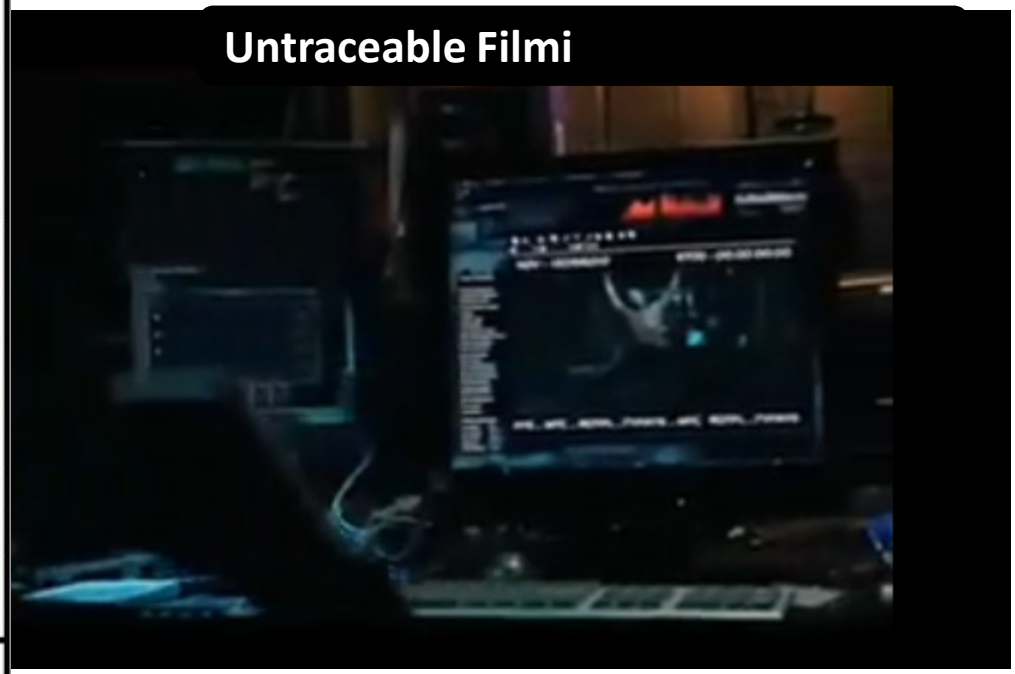
BotNet Satın Alma



FastFlux Networks

- Domain isimlerinin düşük TTL kullanılarak binlerce farklı IP adresi üzerinden sunulması





FastFlux Networks-Örnek

1	97.81.100.62	banner82.com	cookie68.com
2	84.10.100.196	ns1.exportpe.net	ns1.cookie68.com
3	70.231.150.161	ns3.exportpe.net	ns3.cookie68.com
4	89.78.235.81	ns4.exportpe.net	ns4.cookie68.com
5	89.78.235.81	ns4.exportpe.net	ns4.cookie68.com
6	68.154.33.242	banner82.com	ns6.cookie68.com
7	12.73.196.171	banner82.com	ns7.cookie68.com
8	98.200.11.115	banner82.com	ns8.cookie68.com
9	97.80.36.252	banner82.com	cookie68.com
10	12.73.196.171	banner82.com	cookie68.com
11	24.31.142.111	banner82.com	cookie68.com
12	216.234.125.155	banner82.com	cookie68.com
13	99.227.84.105	banner82.com	cookie68.com
14	83.5.252.66	banner82.com	cookie68.com
15	69.140.230.80	banner82.com	cookie68.com
16	98.200.11.115	banner82.com	cookie68.com
17	68.154.33.242	banner82.com	cookie68.com
18	97.81.100.62	banner82.com	ns8.cookie68.com
19	83.5.252.66	banner82.com	ns8.cookie68.com
20	68.154.33.242	banner82.com	ns8.cookie68.com
21	216.234.125.155	banner82.com	ns8.cookie68.com
22	69.140.230.80	banner82.com	ns8.cookie68.com
23	12.73.196.171	banner82.com	ns8.cookie68.com
24	99.227.84.105	banner82.com	ns8.cookie68.com
25	97.80.36.252	banner82.com	ns8.cookie68.com
26	24.31.142.111	banner82.com	ns8.cookie68.com
27	12.73.196.171	banner82.com	ns6.cookie68.com
28	24.31.142.111	banner82.com	ns6.cookie68.com
29	98.200.11.115	banner82.com	ns6.cookie68.com
30	97.80.36.252	banner82.com	ns6.cookie68.com
31	83.5.252.66	banner82.com	ns6.cookie68.com
32	216.234.125.155	banner82.com	ns6.cookie68.com
33	69.140.230.80	banner82.com	ns6.cookie68.com
34	99.227.84.105	banner82.com	ns6.cookie68.com
35	97.81.100.62	banner82.com	ns6.cookie68.com
36	83.5.252.66	banner82.com	ns7.cookie68.com
37	69.140.230.80	banner82.com	ns7.cookie68.com

DOS hakkında yanlış bilinenler

- Bizim Firewall DOS'u engelliyor
- Bizim IPS DOS/DDOS'u engelliyor...
- Linux DOS'a karşı dayanıklıdır
- Biz de DDOS engelleme ürünü var
- Donanım tabanlı firewallar DOS'u engeller
- Bizde antivirüs programı var

- DOS/DDOS Engellenemez

Amaç?

- Sistemlere sızma girişimi değildir!!
- Bilgisayar sistemlerini ve bunlara ulaşım yollarını işlevsiz kılmak
- Web sitelerinin ,

E-postaların, telefon

sistemlerinin çalışmaması

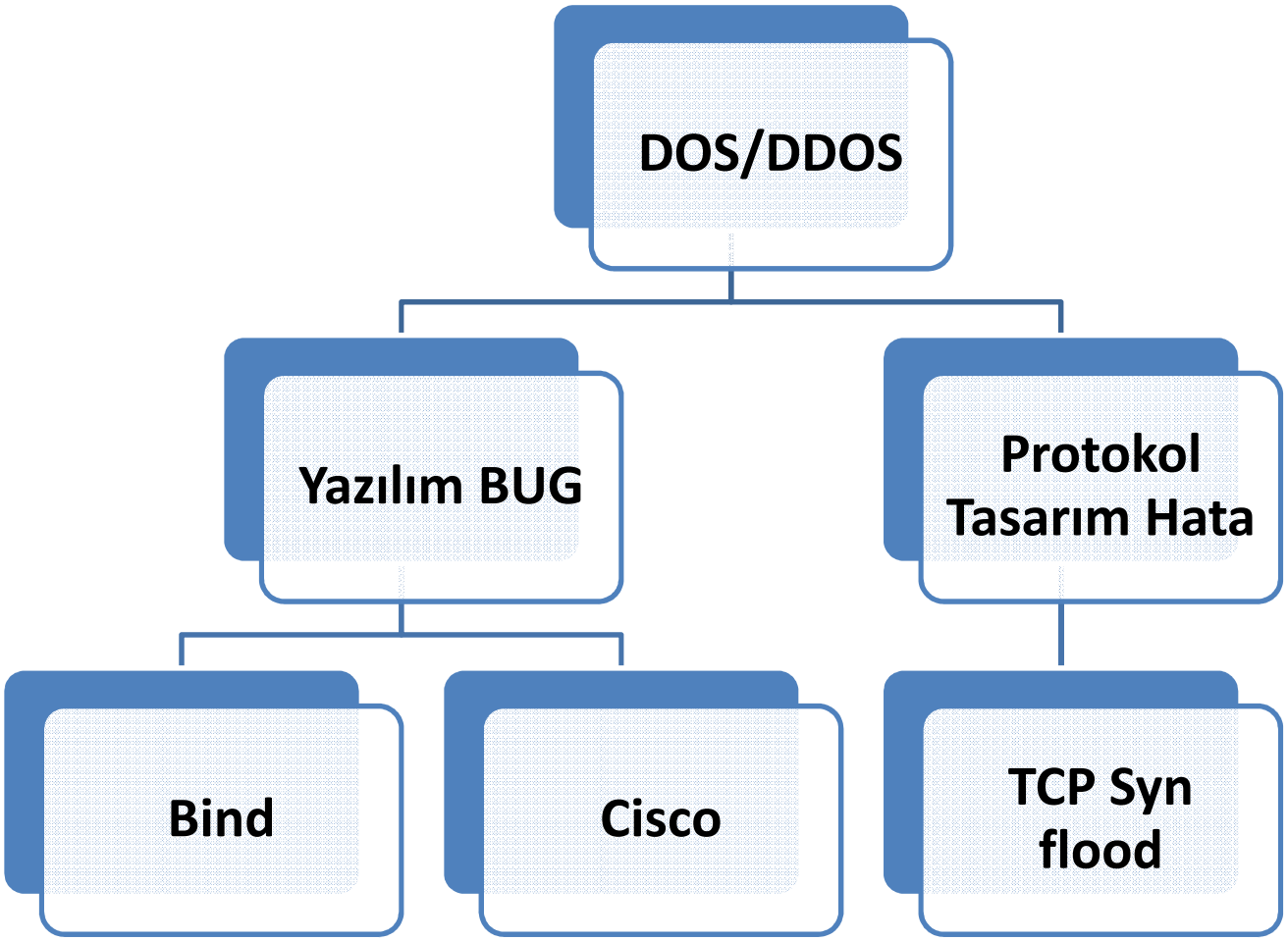
Kim/kimler yapar?

- Hacker grupları
- Devletler
- Sıradan kullanıcılar

Niye yapılır?

- Sistemde güvenlik açığı bulunamazsa zarar verme amaçlı yapılabilir
- Politik sebeplerden
- Ticari sebeplerle
- Can sıkıntısı & karizma amaçlı
  - Bahis amaçlı(forumlarda)

Neden kaynaklanır?



DDOS Sonuçları

Antivirüs Programları korur mu?

a-squared	4.0.0.101	2009.05.15	-
AhnLab-V3	5.0.0.2	2009.05.15	-
AntiVir	7.9.0.168	2009.05.15	TR/Crypt.XPACK.Gen
Antiy-AVL	2.0.3.1	2009.05.15	-
Authentium	5.1.2.4	2009.05.15	-
Avast	4.8.1335.0	2009.05.15	Win32:MDrop-A
AVG	8.5.0.336	2009.05.15	Dropper.Mdrop.N
BitDefender	7.2	2009.05.15	-
CAT-QuickHeal	10.00	2009.05.15	-
ClamAV	0.94.1	2009.05.15	-
Comodo	1157	2009.05.08	-
DrWeb	5.0.0.12182	2009.05.15	-
eSafe	7.0.17.0	2009.05.14	-
eTrust-Vet	31.6.6507	2009.05.15	-
F-Prot	4.4.4.56	2009.05.15	-
F-Secure	8.0.14470.0	2009.05.15	-
Fortinet	3.117.0.0	2009.05.15	-
GData	19	2009.05.15	Win32:MDrop-A
Ikarus	T3.1.1.49.0	2009.05.15	-
K7AntiVirus	7.10.735	2009.05.14	-
Kaspersky	7.0.0.125	2009.05.15	-
McAfee	5616	2009.05.15	-
McAfee+Artemis	5616	2009.05.15	-
McAfee-GW-Edition	6.7.6	2009.05.15	Trojan.Crypt.XPACK.Gen
Microsoft	1.4602	2009.05.15	-
NOD32	4080	2009.05.15	-
Norman	6.01.05	2009.05.14	-

Dünyadan DOS/DDOS Örnekleri

Distributed denial of service attacks on root nameservers

From Wikipedia, the free encyclopedia

Distributed denial of service attacks on root nameservers are several significant Internet events in which distributed denial-of-service attacks have targeted one or more of the thirteen Domain Name System root nameservers. The root nameservers are a critical infrastructure components of the Internet, mapping domain names to Internet Protocol (IP) addresses and other information. Attacks against the root nameservers can impact operation of the entire Internet, rather than specific websites.

Contents [hide]

1 Attacks
- 1.1 October 21, 2002
- 1.2 February 6, 2007

2 References

3 External links

Attacks [edit]

October 21, 2002 [edit]

On October 21, 2002 an attack, lasting for approximately one hour, was targeted at all 13 DNS root name servers.[1]

This event was the first significant attack directed at trying to disable the Internet itself, instead of specific websites.[*citation needed*] This was the second significant failure of the root nameservers; the first large malfunction of them caused the failure of seven machines in April 1997, due to a technical problem.[2]

February 6, 2007 [edit]

On February 6, 2007, an attack began at 10:00 UTC and lasted twenty-four hours. At least two of the root servers reportedly *suffered badly* (G-ROOT and L-ROOT), while two others experienced *heavy traffic* (F-ROOT and M-ROOT). The latter two largely contained the damage by distributing requests to other root server instances with anycast addressing. ICANN published a formal analysis shortly after the event.[3] Due to some lack of detail, speculation about the incident proliferated in the press until details were released.[4]

On February 8, 2007 it was announced by Network World that "*If the United States found itself under a major cyberattack aimed at undermining the nation's critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch an actual bombing of an attack source or a cyber counterattack.*"[5]

Dünyadan DDOS Örnekleri

Georgia DDoS Attacks – A Quick Summary of Observations

by Jose Nazario

The clashes between Russia and Georgia over the region of South Ossetia have been shadowed by attacks on the Internet. As we noted in July, the Georgia presidential website fell victim to attack during a war of words. A number of DDoS attacks have occurred in the region, and often do when tensions flare. We have been observing the attacks, making measurements, and sharing data with a select group of others to trace the origins of the attacks and monitor the situation.

While some are speculating about cyber-warfare and state sponsorship, we have no data to indicate anything of the sort at this time. We are seeing some botnets, some well known and some not so well known, take aim at Georgia websites. Note that RIA Novosti, a Russian news outlet, was apparently targeted during this fighting. Georgian hackers are accused of this event.

Compared to the May 2007 Estonian attacks, these are more intense but have lasted (so far) for less time. This could be due to a number of factors, including more sizable botnets with more bandwidth, better bandwidth at the victims, changes in our observations, or other factors.

Below are some observations of the attacks based on our Internet statistics collection. These are observed attacks, ones that triggered alarms. We know that not all attacks are accounted for here, only many of the major ones. These attacks were mostly TCP SYN floods with one TCP RST flood in the mix. No ICMP or UDP floods detected here. These attacks were all globally sourced, suggesting a botnet (or multiple botnets) were behind them.

Number of attacks	Destination
5	213.131.44.138
3	213.157.196.25
10	213.157.198.33
1	www.gazeti.ge

Raw statistics of the attack traffic paint a pretty intense picture. We can discern that the attacks would cause injury to almost any common website.

Average peak bits per second per attack	211.66 Mbps
Largest attack, peak bits per second	814.33 Mbps
Average attack duration	2 hours 15 minutes
Longest attack duration	6 hour

Dünyadan DDOS Örnekleri

Estonian DDoS Attacks – A summary to date

by Jose Nazario

Time sure flies. I looked up from working and noticed I hadn't blogged in a while. And I noticed that I hadn't been analyzing the Estonian DDoS attacks in a week or two.

ATLAS gives us an amazing view into the Internet's activities. ATLAS collects DoS attack data from around the world through sharing arrangements and even from some of our Peakflow SP deployments. As such, the recent DDoS attacks on Estonia are visible, in part, from within ATLAS. I've always had a soft spot in my heart for Estonia. Since the fall of the Iron Curtain, it's become technically advanced, society has done wonders to improve itself and it's jumped, quite successfully, into the modern world. It has a nearly model economy, based in large part on the teachings of Milton Friedman who favored free markets unfettered by state control.

As you can imagine, having development access to the ATLAS data repository allows me to build new reports and crunch the data in new and exciting ways. I analyzed about 2 weeks of DDoS attacks on Estonia this morning using internal tools and reporting systems, and here's what I found.

We've seen 128 unique DDoS attacks on Estonian websites in the past two weeks through ATLAS. Of these, 115 were ICMP floods, 4 were TCP SYN floods, and 9 were generic traffic floods. Attacks were not distributed uniformly, with some sites seeing more attacks than others:

Attacks	Destination	Address or owner
35	"195.80.105.107/32"	pol.ee
7	"195.80.106.72/32"	www.riigikogu.ee
36	"195.80.109.158/32"	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	"195.80.124.53/32"	m53.envir.ee
2	"213.184.49.171/32"	www.sm.ee
6	"213.184.49.194/32"	www.agri.ee
4	"213.184.50.6/32"	
35	"213.184.50.69/32"	www.fin.ee (Ministry of Finance)
1	"62.65.192.24/32"	

The attacks themselves haven't been steady, at least from the perspective given by ATLAS. If we look at how many attacks occurred on every day, we can see that they peaked a week or so ago, but they haven't necessarily stopped.

Dünyadan DOS Örnekleri

Web Attacks Expand in Iran's Cyber Battle (Updated Again)

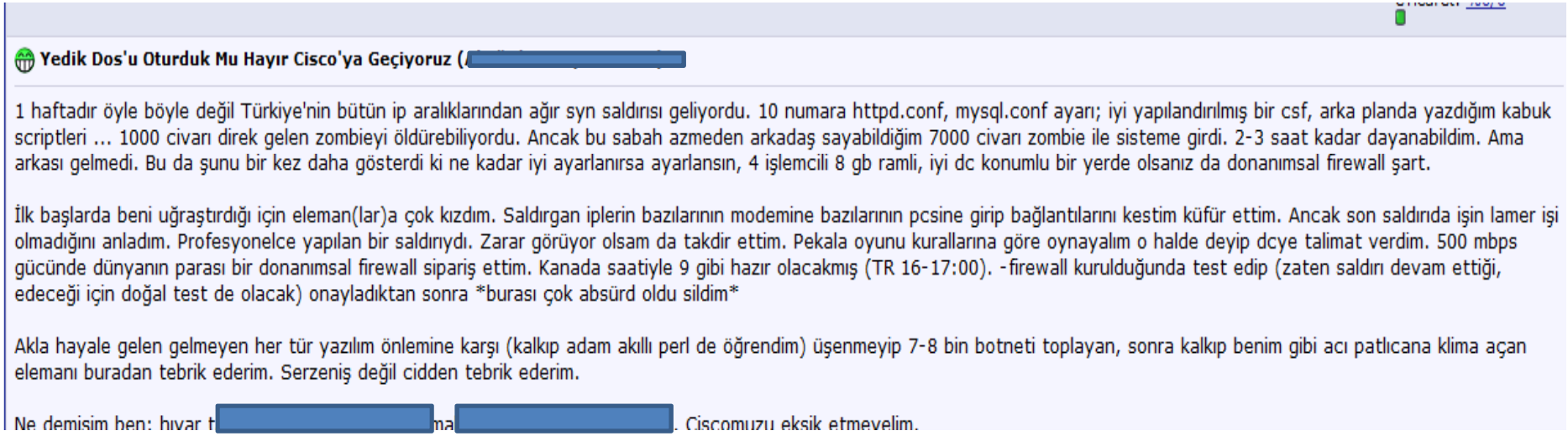
By Noah Shachtman ✉ June 16, 2009 | 4:06 pm | Categories: Info War, Rogue States

More and more of Iran's pro-government websites are under assault, as opposition forces launch web attacks on the Tehran regime's online propaganda arms.

What started out as an attempt to overload a small set of official sites has now expanded, network security consultant Dancho Danchev notes. News outlets like Raja News are being attacked, too. The semi-official Fars News site is currently unavailable.

"We turned our collective power and outrage into a serious weapon that we could use at our will, without ever having to feel the consequences. We practiced distributed, citizen-based warfare," writes Matthew Burton, a former U.S. intelligence analyst who joined in the online assaults, thanks to a "push-button tool that would, upon your click, immediately start bombarding 10 Web sites with requests."

Türkiye’den DDOS Örnekleri



Yedik Dos'u Oturduk Mu Hayır Cisco'ya Geçiyoruz ([redacted]

1 haftadır öyle böyle değil Türkiye'nin bütün ip aralıklarından ağır syn saldırısı geliyordu. 10 numara httpd.conf, mysql.conf ayarı; iyi yapılandırılmış bir csf, arka planda yazdığım kabuk scriptleri ... 1000 civarı direk gelen zombieyi öldürebiliyordu. Ancak bu sabah azmeden arkadaş sayabildiğim 7000 civarı zombie ile sisteme girdi. 2-3 saat kadar dayanabildim. Ama arkası gelmedi. Bu da şunu bir kez daha gösterdi ki ne kadar iyi ayarlanırsa ayarlansın, 4 işlemcili 8 gb ramli, iyi dc konumlu bir yerde olsanız da donanımsal firewall şart.

İlk başlarda beni uğraştırdığı için eleman(lar)a çok kızdım. Saldırgan iplerin bazılarının modemine bazılarının pcsine girip bağlantılarını kestim küfür ettim. Ancak son saldırıda işin lamer işi olmadığını anladım. Profesyonelce yapılan bir saldırıydı. Zarar görüyor olsam da takdir ettim. Pekala oyunu kurallarına göre oynayalım o halde deyip dcye talimat verdim. 500 mbps gücünde dünyanın parası bir donanımsal firewall sipariş ettim. Kanada saatiyle 9 gibi hazır olacakmış (TR 16-17:00). -firewall kurulduğunda test edip (zaten saldırı devam ettiği, edeceği için doğal test de olacak) onayladıktan sonra *burası çok absürd oldu sildim*

Akla hayale gelen gelmeyen her tür yazılım önlemine karşı (kalkıp adam akıllı perl de öğrendim) üşenmeyip 7-8 bin botneti toplayan, sonra kalkıp benim gibi acı patlıcana klima açan elemanı buradan tebrik ederim. Serzeniş değil cidden tebrik ederim.

Ne demişim ben: hıyar t[redacted]ma[redacted]. Ciscomuzu eksik etmeyelim.

Türkiye’den DDOS Örnekleri

Teklan ile Siberalem Arasında dDOS Tartışması

EBI firması, kendisine dDOS saldırısı yapıldığı suçlamasıyla Teklan aleyhine beyoğlu Cumhuriyet Savcılığına şikayette bulundu. Şirketin itiraf.com, siberalem benzeri sitelerinin host edildiği firma olan Teklan'dan ayrılmak istemesi üzerine saldırıların başladığı iddiası, sektörü karıştırdı. Teklan konuyla ilgili bir açıklama yaparak, olayı yalanladı.

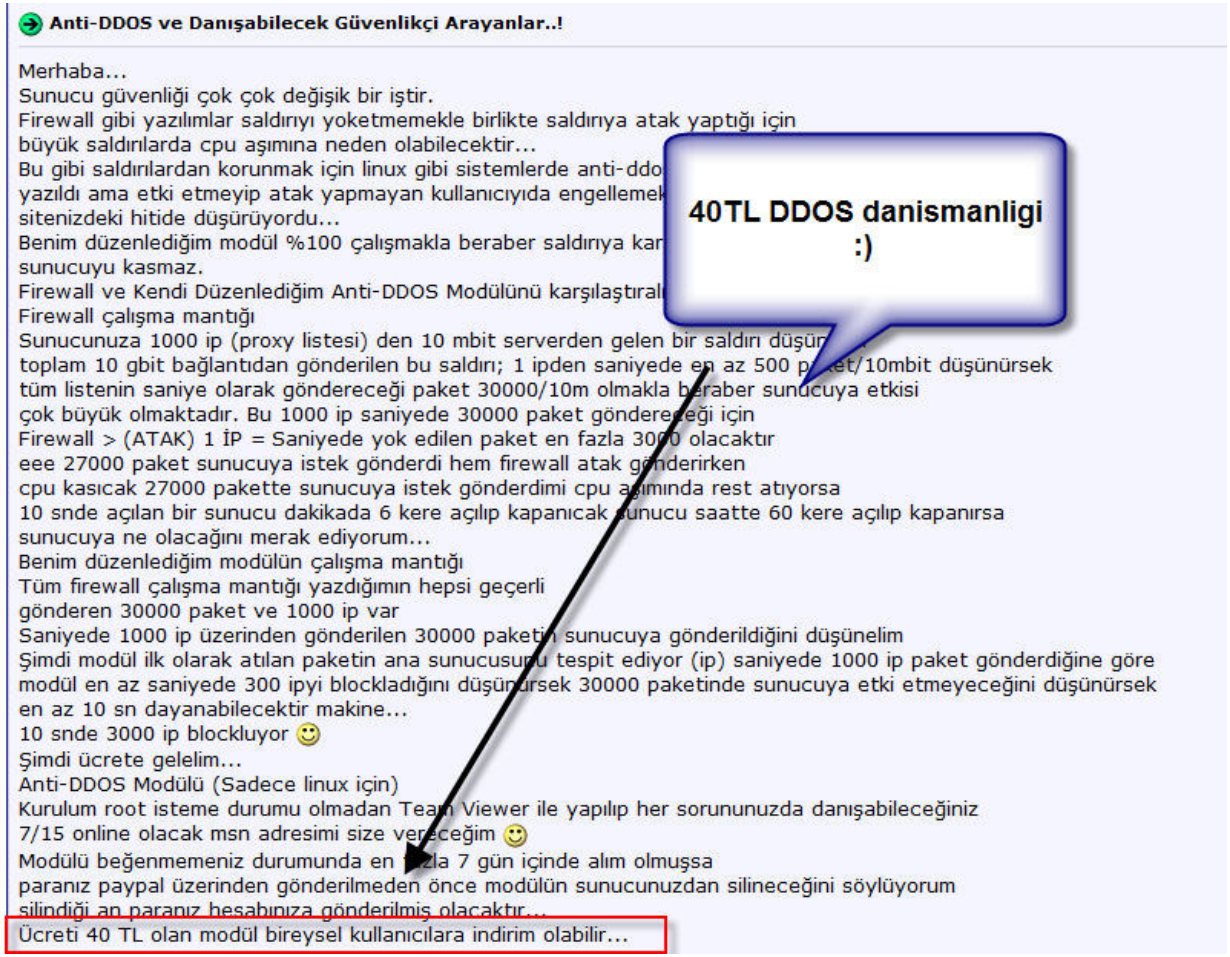
İnternet kullanımı geliştikçe, internetle ilgili yeni kavramlar ve olaylarla karşılaşılıyor. İşte bunlardan birisi de dDos saldırıları. Saldırı yapılan sunucuları, o sunucunun ya da kullandığı bant genişliğinin kapasitesinin üstünde talep yaparak, çöktürmek anlamına gelen Ddos saldırıları, ilk olarak Microsoft’a ve daha sonra San Fransisco’daki internet kök sunuculara yapılan büyük saldırılarla gündemimize girmişti.

İşte bu konuda ilginç bir olay İstanbul’da meydana geldi. İnternet’in popüler arkadaşlık (sosyal network)portallerinden SiberAlem’in temmuz ayı içinde uğradığı Ddos saldırıları sonucunda, sistemin 5-6 gün gibi uzun süreler boyu kullanılamaz hale gelmesi sonucu adli makamlara şikayette bulunduğu ve yapılan tespitler sonucu da Teklan'ın birlikte çalıştığı, dakikhost firmasından bir kişinin gözaltına alındığı ve sonra tutuksuz yargılanmak üzere hakkında dava açıldığı, ayrıca Teklan yöneticilerinin de ifadelerinin alınacağı bilgisini aldık.

Konuyla ilgili iddia, Teklan ile SiberAlem sitesinin sahibi olan EBI arasında bir iş anlaşmazlığı olduğu şeklinde. Sitenin host edildiği Teklan firmasının dönem sonunda, büyük bir hosting ücreti istemesi üzerine, EBI’nin hosting firmasını değiştirmeye karar vermesinin, Teklan tarafından hoş karşılanmadığı ve bunun üzerine de saldırıların yapılmaya başlandığı iddiası ile yapılan şikayet dün internet camiasına bomba gibi düştü.

Gerçi konu, internet camiasında bir süredir zaten konuşuluyordu. Çünkü dDOS saldırısının, portalin daha sonra taşındığı Netone firmasının da rahatsız ettiği biliniyor. Ayrıca geçtiğimiz günlerde yayına başlayan ve futbol maçlarını video ile veren portal gibi bir kaç sitenin de saldırıya uğradığı konuşuluyor.

Türkiye’den DDOS Örnekleri

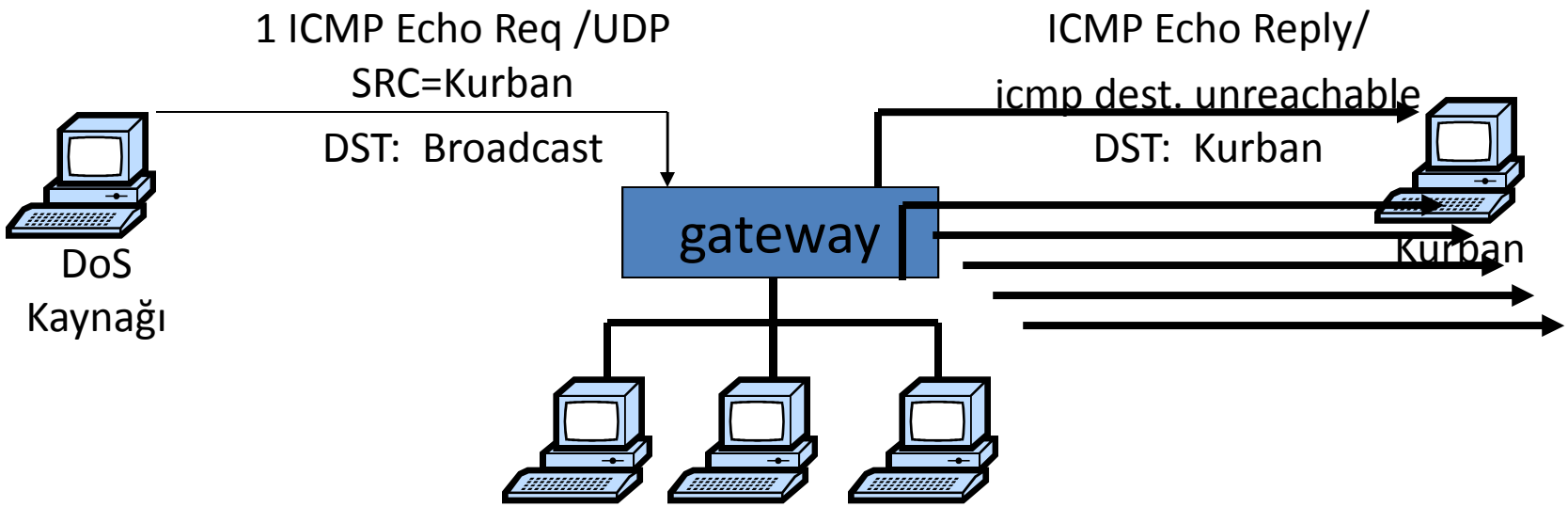


DOS/DDOS Çeşitleri

- Amaca göre DDOS Çeşitleri
  - Bandwith tüketimi
  - Kaynak tüketimi(CPU, RAM, disk vs)
- Yapılış şekline göre DOS/DDOS çeşitleri
- ARP, Wireless
- IP
- ICMP
- TCP
- UDP
- DHCP/SMTP/HTTP/HTTPS/DNS

Eski yöntemler:Smurf atağı

ICMP ve UDP Paketleri Broadcast olarak gönderilebilir



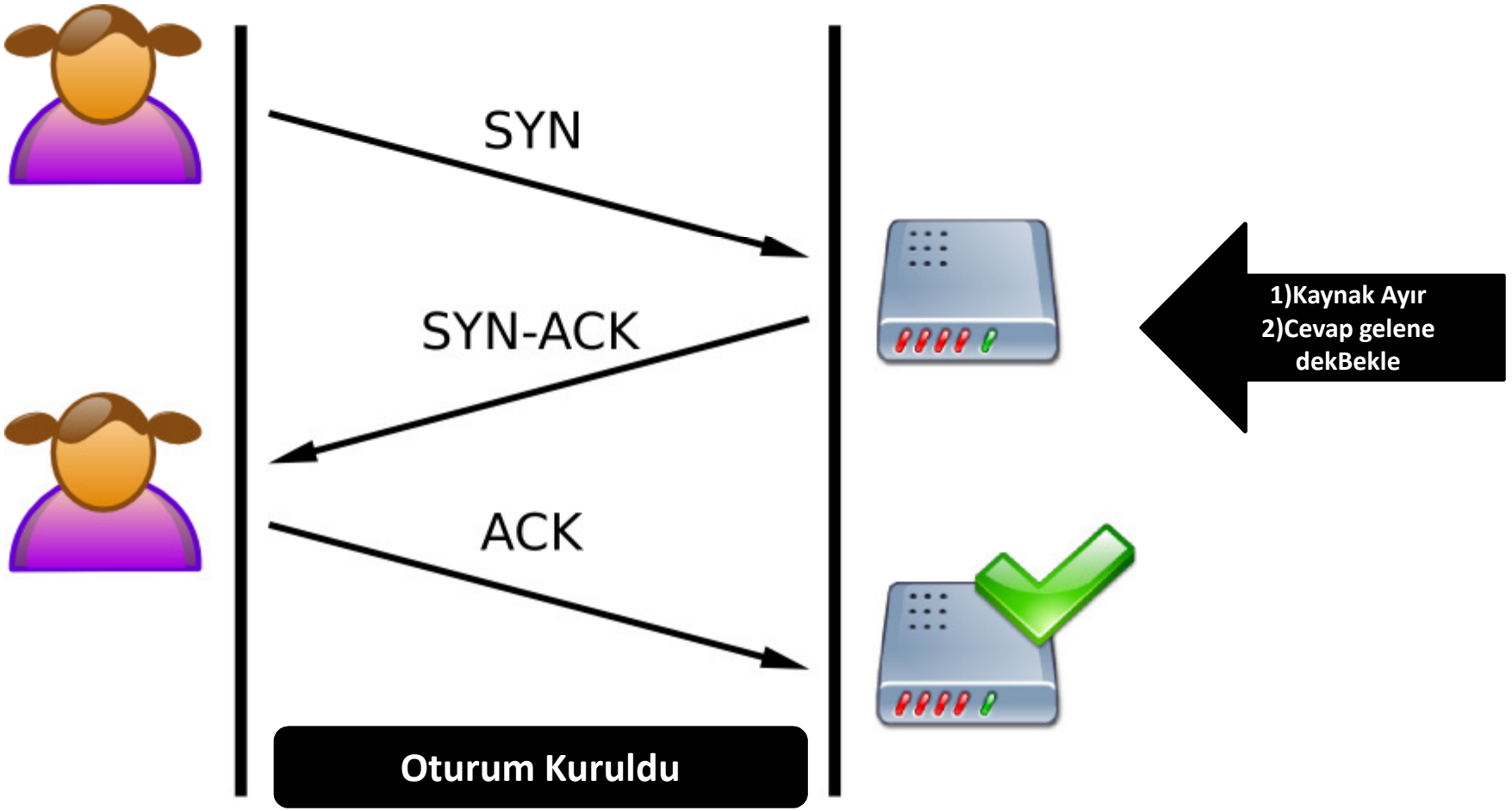
Tek bir paket gönderilerek milyonlarca cevap dönülmesi sağlanabilir(di)

Günümüzde tercih edilen yöntemler

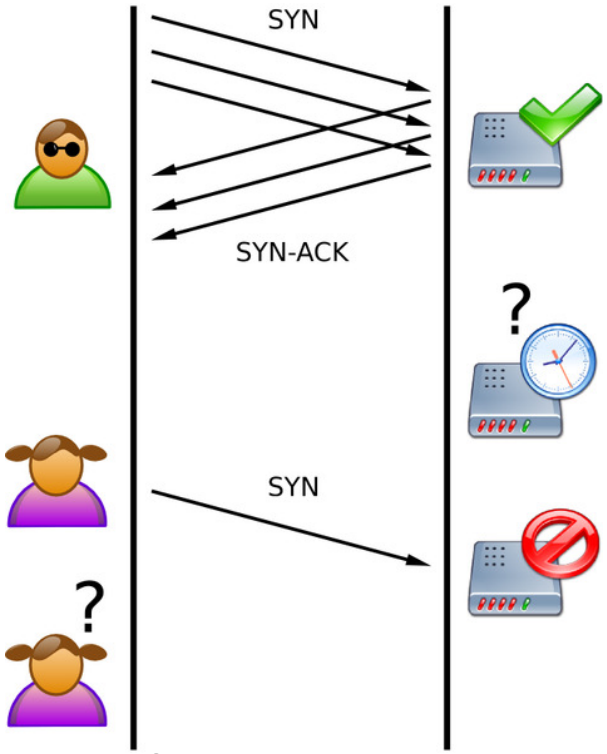
- SYN Flood
- HTTP Get / Flood
- UDP Flood
- DNS DOS
- Amplification DOS saldırıları
- BGP Protokolü kullanarak DOS
- Şifreleme-Deşifreleme DOS saldırıları

SYN Flood Saldırıları

- Normal TCP İşleyişi



SYN Flood



120 saniye bekler

- Bir SYN paketi ortalama 65 Byte
- 8Mb ADSL sahibi bir kullanıcı saniyede 16.000 SYN paketi üretebilir, 10 ADSL kullanıcısı?

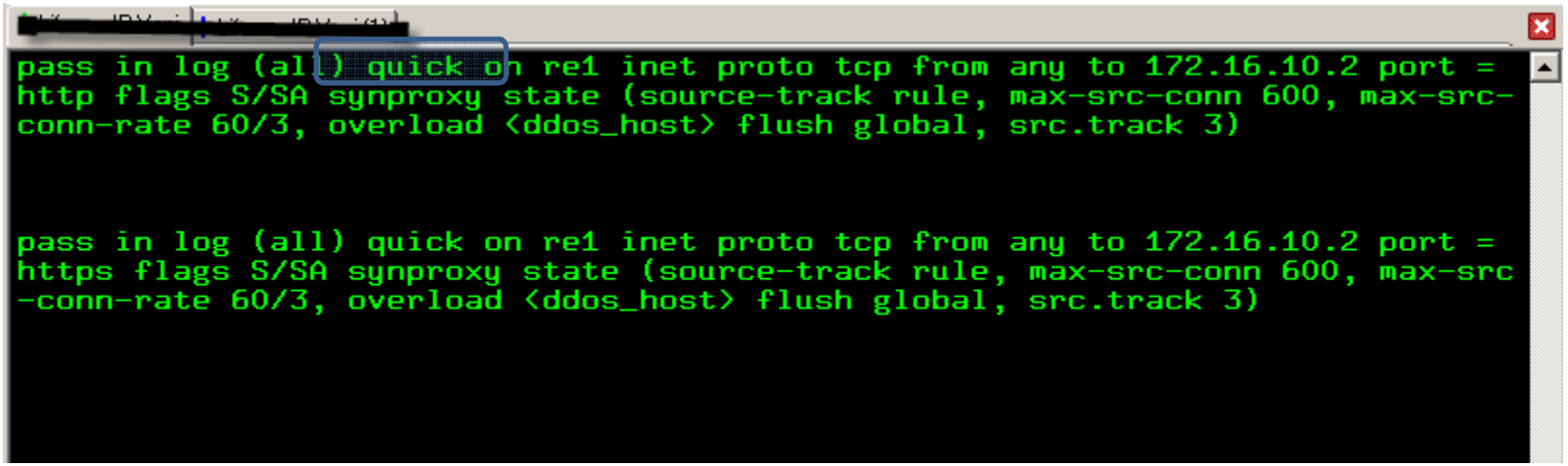
SYN Flood Koruma-1

- Tcp timeout değerlerini düşürme

```
TIMEOUTS:
tcp.first                  120s
tcp.opening                 30s
tcp.established          86400s
tcp.closing                900s
tcp.finwait                 45s
tcp.closed                  90s
tcp.tsdiff                  30s
udp.first                   60s
udp.single                  30s
udp.multiple                60s
icmp.first                  20s
icmp.error                  10s
other.first                 60s
other.single                30s
other.multiple              60s
frag                        30s
interval                    10s
adaptive.start           60000 states
adaptive.end            120000 states
src.track                    0s
```

Syn Flood Koruma-II

- TCP servisleri önüne güvenlik duvarı koyma
- Syn cookies özelliği kullanma
- Syncache mekanizması
- Syn proxy mekanisması



SynCookie Mantığı

- Amaç: Kandırılmış ip adreslerinden gelen SYN paketleri için kaynak harcamamak
- Bunun için belirli zaman geçerli olacak cookiler üretilerek SQN olarak gönderilir.
- Dönen ACK cevapları(dönerse) tekrar cookie mantığıyla kontrol edilip kabul edilir.
- Dezavantajı:Yüklü SYN flood saldırılarında kriptografik işlemlerden dolayı CPU performans problemi.

SYN Cookie Alt etme

- Sunucu tarafında kullanılan syncookie özelliği istemci tarafında da kullanılarak sunucudaki syncookie özelliği işe yaramaz hale getirilebilir.
- Böylece istemci kendi tarafında state tutmaz, sunucu tarafında da 3'lü el sıkışma tamamlandığı için bağlantı açık kalır(uzuun süre)
- Sockstress, scanrand araçları

UDP Flood Saldırıları

- UDP=Connectionless bir protokol
  - IP spoofing yapılabilir
  - hping –udp www.lifeoverip.net -p 53 -a www.microsoft.com
  - Paket boyutu ~ 30 byte
  - 20Mb hat ile saniyede 90.000 pps üretilebilir.
    - 20*1024*1024/8/30
  - UDP bağlantısının kapatılması için gerekli ortlama süre 60 saniye...

UDP Flood saldırıları

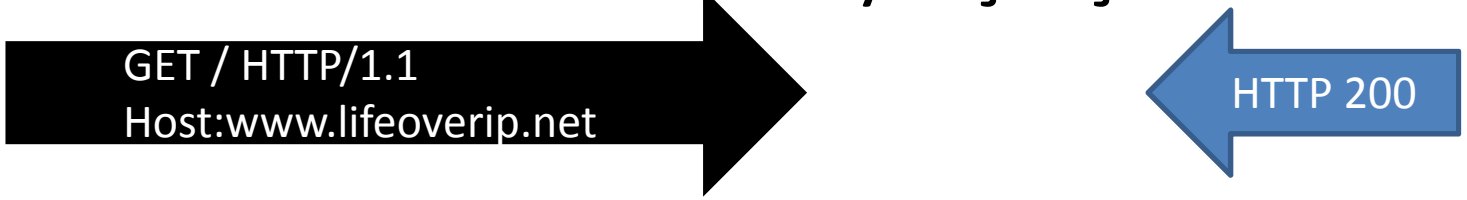
- Rastgele üretilmiş sahte ip adreslerinden saniyede 90.000 paket. Her paket için 60 saniye bekleme süresi
- Piyasadaki çoğu Firewall/IPS ürününün kapasitesinin üzerinde

UDP Flood Saldırılarından korunma

- Daha güçlü güvenlik duvarları
- Belirli ip adresinden gelecek istekleri sınırlama
- Timeout değerlerini düşürme
  - 60 saniyeden 10 saniyeye düşürülebilir(saldırı anında)

HTTP Üzerinden Yapılan DOS/DDOS

- HTTP(Hypertext Transfer Protocol)
  - Web sayfalarını ziyaret ederken kullanılan protokol
- HTTP istek ve cevaplarıyla çalışır



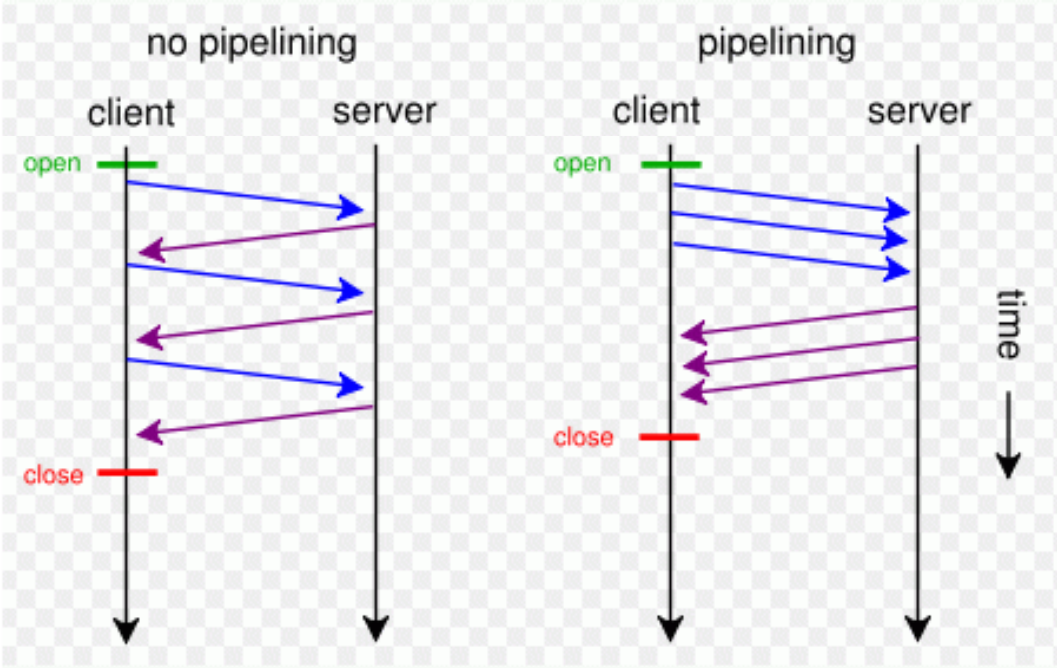
- Web sunucuların belirli kapasitesi vardır
  - Eş zamanlı 500 istek kabul et gibi
- Bir kullanıcı tek bilgisayardan eş zamanlı 500 istek yapabilir

HTTP Çalışma Yapısı

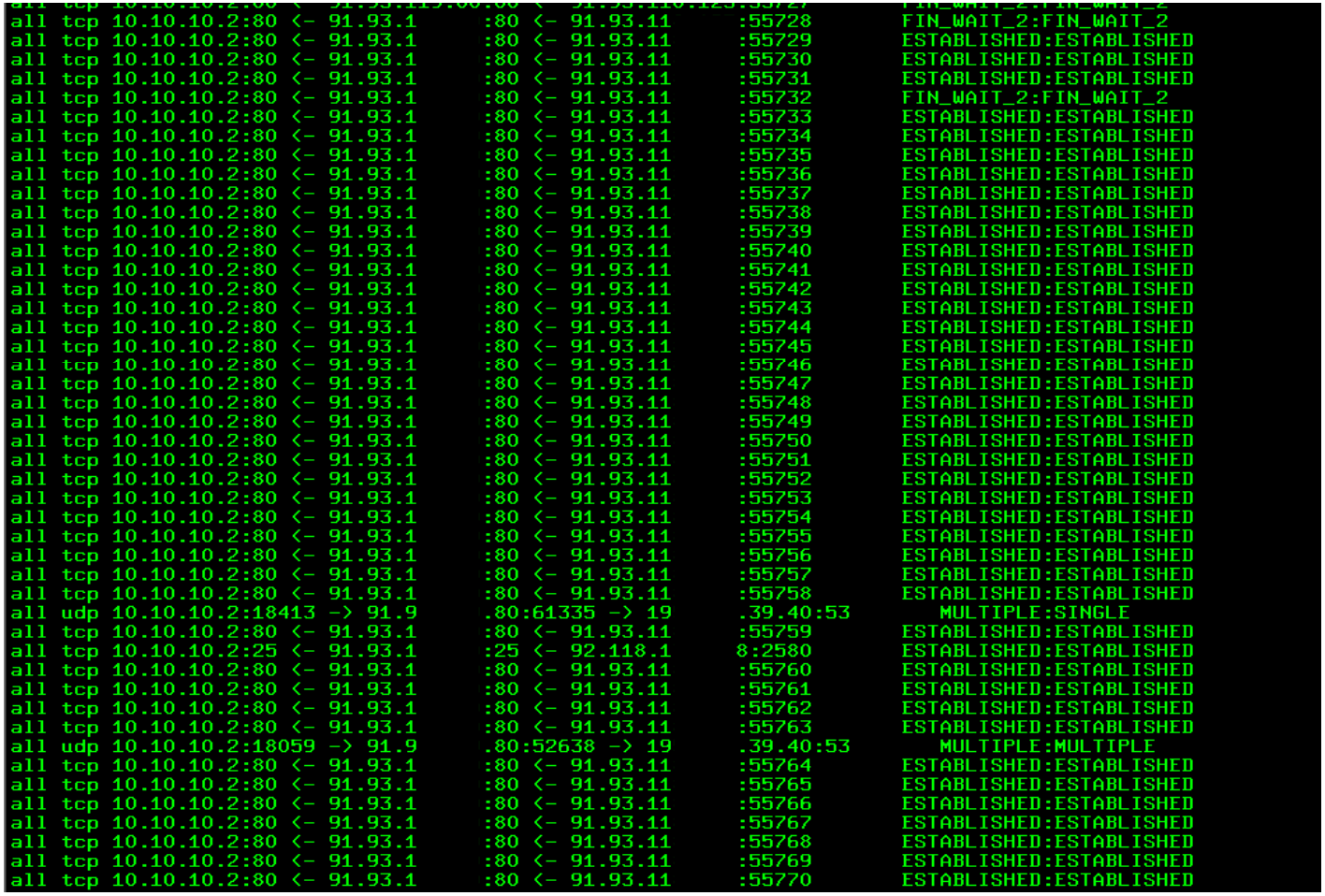
- Garip bir protokol
  - Bir sayfaya girmek için ortalama 50-60 istek gönderilir. Her istek ortalama 6 pakettir(syn, ack, fin)
  - Bu istekler birbirinden bağımsızdır.
  - 100 kişi aynı anda ana sayfaya girse toplamda 30.000 istek oluşur bu da sunucu tarafında performans sıkıntısı demektir.
- Performans sıkıntısına önlem: Keep Alive mekanizması

HTTP KeepAlive

Sunucudan istenecek her isteğin ayrı bir TCP bağlantısı yerine tek bir TCP bağlantısı üzerinden gönderilmesi sağlanabilir.



HTTP Üzerinden DOS



Snort ile HTTP Flood saldırıları Engelleme

- Mantık basit: HTTP sunucuya gelebilecek HTTP isteklerini ip bazında sınırlama(TCP seviyesinde değil)
- Her ip den anlık gelebilecek max HTTP GET/HEAD/POST isteği=100

```
alert tcp any any -> any  80 (msg:"HTTP GET Flood Attack  Attempt"; content:"GET";
nocase; depth:10; detection_filter: track by_src, count 90, seconds 3; sid:1000001;
 rev:1;)
```

DNS Servisine yönelik DDOS Saldırıları

- DNS UDP üzerinden çalışır= kandırılmaya müsait servis
- DNS = Internet'in en zayıf halkası
  - E-posta hizmetleri
  - Web sayfalarının çalışması
  - İnternetim çalışmıyor şikayetinin baş kaynağı ☺
- DNS sunuculara yönelik DDOS saldırıları
  - DNS yazılımında çıkan buglar
  - ENDS kullanımı ile amplification saldırıları
  - DNS sunucuların kapasitelerini zorlama

DNS Sunucularda çıkan buglar ve DOS

Internetin %80 ISC Bind yazılımı kullanıyor

Yıl 2009 ...

/// File Name:	solinger.c
Description:	"solinger" Denial Of Service - BIND 8.1.*, 8.2, 8.2.1 - causes a BIND8 server to stop responding to requests for up to 120 seconds. Quick proof of concept of the bug pointed out by ISC.
Author:	Mixter
Homepage:	http://mixter.void.ru
MD5 Checksum:	0969c6c7e46e8710f57450bca51ed6af

/// File Name:	CSSA-1999-034.0.txt
Description:	Caldera Advisory - Several vulnerabilities have been discovered involves a buffer overflow that can possibly be used by a skilled
MD5 Checksum:	f372b37e400da08fae2dd765c7d715ce

/// File Name:	bind.nxt.txt
Description:	A bug in the processing of NXT records allows attackers remot detailed information about the bug and the handling of NXT rec
MD5 Checksum:	6f9bfe05817ae7378fd260502ace3530

/// File Name:	named_dump.sh
Description:	ISC BIND 4.9.7-T1B local exploit - The named daemon will dun any file in the system.
Homepage:	http://www.hack.co.za
MD5 Checksum:	9e3322da75b9792e0a877bdaabb9a82f

/// File Name:	bind8x.c
Description:	BIND prior to 8.2.3-REL remote root exploit - exploits the name
Author:	lx,Lucysoft
MD5 Checksum:	c4f9cc6d4b7bc657ff22984adf7d206c

/// File Name:	sms.203.ypbind
Description:	Sun Microsystems Security Bulletin #203 - The ypBIND daemo remote attacker to gain root access. Vulnerable systems includ
Homepage:	http://sunsolve.sun.com/security
MD5 Checksum:	46e0491127139c68520874f9000b1129

BIND Dynamic Update DoS

CVE:	CVE-2009-0696
CERT:	VU#725188
Posting date:	2009-07-28
Program Impacted:	BIND
Versions affected:	BIND 9 (all versions)
Severity:	High
Exploitable:	remotely
Summary:	BIND denial of service (server crash) caused by receipt of a specific remote dynamic update message.

Description:

Urgent: this exploit is public. Please upgrade immediately.

Receipt of a specially-crafted dynamic update message to a zone for which the server is the master may cause BIND 9 servers to exit. Testing indicates that the attack packet has to be formulated against a zone for which that machine is a master. Launching the attack against slave zones does not trigger the assert.

This vulnerability affects all servers that are masters for one or more zones – it is not limited to those that are configured to allow dynamic updates. Access controls will not provide an effective workaround.

dns_db_findrdataset() fails when the prerequisite section of the dynamic update message contains a record of type "ANY" and where at least one RRset for this FQDN exists on the server.

```
db.c:659: REQUIRE(type != ((dns_rdatatype_t)dns_rdatatype_any)) failed
exiting (due to assertion failure).
```

Workarounds:

BIND Dynamic Update DoS

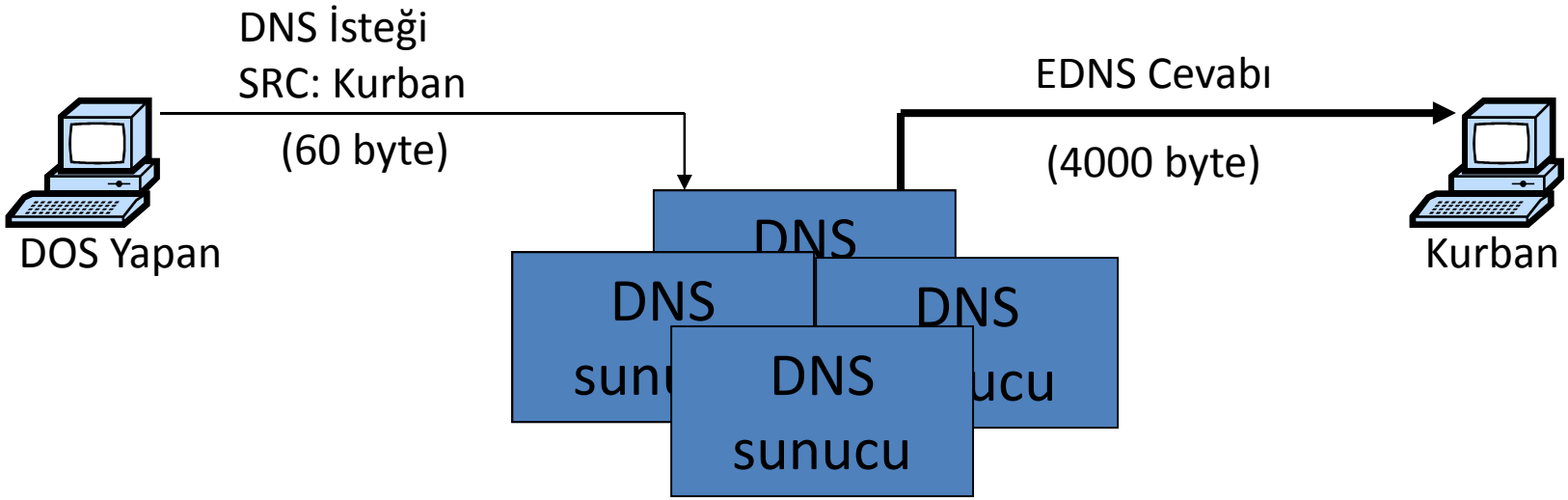
- ISC bind 2009 Temmuz
- Bu tarihe kadarki tüm bind sürümlerini etkileyen “basit” ama etkili bir araç
- Tek bir paketle Türkiye’nin internetini durdurma(!)
  - Tüm büyük isp’ler bind kullanıyor
  - Dns=udp=src.ip.spoof+bind bug
- %78 dns sunucu bu zaafiyete açık
  - Sistem odalarında nazar boncuğu takılı☺

DNS Amplification Saldırısı

- UDP üzerinden taşınan dns paketleri 512 byten büyük olamaz
- EDNS(RFC 2671) dns sorgularının cevapları 512 bytedan daha büyük olabilir
- 60 byte(dns isteği) gönderip cevap ola byte alınabilir(cevap=56X istek)
- 10Mb bağlantıdan 10X65=650 Mbit tı üretilebilir.
- Koruma: recursive dns sorguları ve edns desteği iyi ayarlanmalı

DNS Amplification DOS

DNS Amplification Saldırısı: (×65 amplification)



Internette herkese açık dns sunucu sayısı ~600,000

DNS sunuculara kaba kuvvet paket saldırısı

- Bir dosya içerisine 1 milyon farklı domain ismi yazılır.
- Paket üreticiler kullanılarak bu domainler hızlıca dns sunucuya spoofed edilmiş ip adreslerinden sorgu olarak gönderilir
- DNS sunucu iyi ayarlanmamışsa gerçek isteklere zaman ayıramaz

BGP Anonslarıyla DOS

- YouTube IP= 208.65.152.0**/22** (2^{10} IP adresi)
  www.youtube.com -> 208.65.153.238, 239..

- Şubat 2008'de:
  - Pakistan telekom youtube yasaklamak için 208.65.153.0**/24** aralığını anons etmeye başladı
  - Spesifik prefixler daha önceliklidir(Routing karar mekanizmasında)
  - Anons sonrası Internet youtube.com'u Pakistan Telekomda sanıyordu
  - 2 saatliğine kesinti
- Önlemi?

DOS Saldırılarını Engelleme

- İlk şart: Sağlam TCP/IP bilgisi
- ISP ile yakın iletişim
- Sınır güvenliğinin ilk halkası routerlar üzerinde
  - Src.port, src ip adresleri belirliyse
- Güvenlik duvarları/IPS'lerin özelliklerini bilme
- Bilinen ddos toollarının default özelliklerini öğrenip doğrudan bloklama
  - Src.port=2043 gibi.
- Kendi sistemlerinizi test edin/ettirin.

DOS Çalışmaları

- Lab Kurulumu
  - 24 portluk 100/1000 switch
  - 3 adet laptop(Linux, Windows yüklü)
  - Test cihazları(Firewall, IPS, Load balancer, Router)
- 1 Laptop+çeşitli araçlar;
  - 600Mbit/s
  - 750.000 pps TCP SYN
  - 800.000 pps UDP

Packet Filter Firewall İle Engelleme

- Güçlü Firewall= 4GB ram=2.000.000 pps (SYN)
- Rate limiting
  - Bir ip adresinden eş zamanlı açılacak bağlantı sayısı
  - Bir ip adresinden toplamda açılabilecek bağlantı(SYN, ACK, RST vs) sayısı
- Kurallarda SYN Proxy kullanımı
- TCP/UDP/ICP timeout değerlerinin düşürülmesi
- HTTP Keepalive kullanılan sistemlerde HTTP Flood saldırılarına karşı koruma yapamaz!

Sonuç

- DOS/DDOS saldırıları internetin en temel sorunlarındandır
- TCP/IP protokolü yapısı iyi bilinirse saldırılar büyük oranda engellenebilir.
- Sadece protokollerin yapısı değil, DDOS'a karşı korunmak istenen network yapısının bilinmesi ve DDOS saldırıları düşünülerek tasarlanması gerekir

DDOS Eğitimleri

DDOS Saldırı Tipleri

DDOS saldırıları Internet dünyasının en eski ve en etkili saldırılarıdır. DDOS saldırılarına karşı kesin bir reçete olamayacağı için bu tip saldırılarlar karşı karşıya kalmadan konu hakkında detaylı bilgi sahibi olmak en büyük silahtır. Konu hakkında bilgi sahibi olmadan alınacak DDOS koruma ürünleri ayrı bir DOS'a(servis kesintisi) sebep olabilmektedir.

Bu eğitimle birlikte sık kullanılan ve etkili olan DDOS yöntemleri, çalışma mantıkları, uygulamaları ve korunma yöntemlerini hem teorik olarak öğrenme hem de pratik olarak görme fırsatı yakalayacaksınız. Eğitmenler Türkiye ve yurt dışında çeşitli firmaların DDOS Testlerini yapmış uzman kişilerden oluşmaktadır.

DDOS Saldırı Tipleri ve Engelleme Yöntemleri Eğitim İçeriği

1.Temel TCP/IP Bilgisi

1. Internetin Altyapısı TCP/IP Protokol Ailesi
2. TCP/IP Ailesi Protokolleri Çalışma Yöntemleri
3. ARP, IP, ICMP, TCP, UDP, DNS, HTTP,SMTP Protokolleri

2.Çözülemeyen Problem DDOS

http://www.guvenlikegitimleri.com

Sorularınız?

- Sunumu: http://www.lifeoverip.net/sunumlar/ddos.pdf adresinden indirebilirsiniz
- huzeyfe@lifeoverip.net adresinden iletişime geçebilirsiniz.
- Http://www.lifeoverip.net/netsec-listesi