

Parola Güvenliği ve Şifre Kırma Saldırıları

Bilgi Güvenliği AKADEMİSİ

Bölüm İçeriği

- Parola Tanımı
- Parola Güvenliğinin Önemi
- Parola Saldırı Çeşitleri
- Windows/Linux/IOS Parola Güvenliği
- Parola Kırma Araçları ve Örnekler

Parola Nedir?

- Günümüz dünyasının güvenlik altyapısının dayandığı zayıf nokta
 - Twitter.com ->whois->xzy@twitter.com->webmail->Username->Password
- Çoklu Kimlik doğrulama ile bu güvensizlik aşılmaya çalışılıyor
- Parola mı Şifre mi?

Şifreleme ve Kodlama

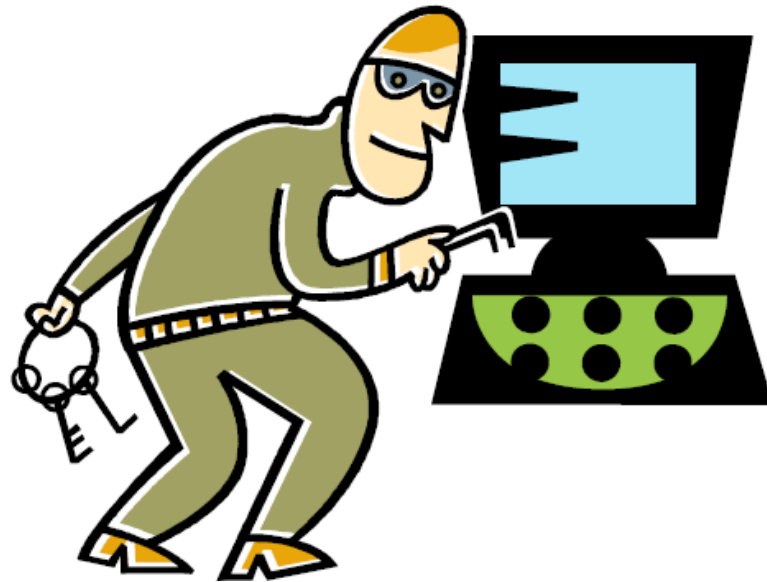
- Şifreleme ile karıştırılan en önemli konulardan birisi encode ve decoding dir
- Kodlama ve çözümlenmede eğer parola elimizde ise ve parolanın kodlanma şeklini biliyorsak çözülmesi çok kolay olacaktır.
- Kodlanmış parola kullanan uygulamalara örnekler:
 - Base64: en sık kullanılan kodlama şeklidir.
 - Cisco tye-7 parolaları.
 - VNC Parolaları

Parola Çeşitleri

- Tek Tip karakter içeren Parolalar
 - Asfendi
 - 12390823
 - #\$%&/
- Karmaşık Parola Tipleri
 - Asfe123di45
 - 12%+&alibaba
 - 3m3ls4y1n
- Passphrase
 - Ben senin beni s3v3b1lme 1ht1malini

Şifreleme Saldırıları

- Pasif Online ataklar
- Aktif Online ataklar
- Offline ataklar



Pasif Online Ataklar

- Network Trafiği dinleyerek elde edilir
- Trafiği dinle
- Authentication aşaması gelince login bilgilerini kaydet
- MITM Yöntemiyle Parolaları toplama

Aktif Online Ataklar

- Web sunuculara, mail sunuculara yönelik ataklar
- Saldırgan hedef bulur
- Hedef parola denemelerine başlar
- Avantajı
 - Kötü parola politikalarında işe yarar
- Dezavantajı
 - İyi seçilmiş parolalarda işe yaramaz
 - Hesap kitleme riski

Offline Ataklar

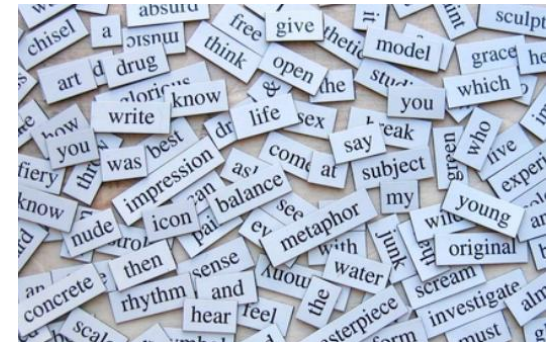
- Öncelikle parolanın şifrelenmiş halde bulunduğu şeyler elde edilmeli
- Sonra çeşitli programlarla offline denemeler yapılır
- WEP/WPA Kırma
- UNIX/Linux/Windows sistemlerin elde edilmiş parolalarının kırılması

Offline Atak tipleri

- Sözlük saldırıları
- Brute force saldırılar
- Hibrid saldırılar
- Rainbow tablo kullanımıyla yapılan saldırılar

Sözlük Saldırıları

- Ortak parola kullanımından kaynaklanır
- Sözlüklerden oluşan bir parola veritabanı oluşturulur
- Her bir sözcük parola olarak denenir
- Avantajı
 - Parola basitse çözüme hızlı ulaşılır
- Dezavantajı
 - Kendi dilinde sözlük oluşturma zorluğu
 - Parola basit değilse bulunamaz



Sözlük Oluşturma

- Her ülkenin, dilin, kültürün ortak kullandığı sözcükler farklıdır
- Kendi sözlüğümüzü nasıl oluşturabiliriz?
- Legal olmayan yol
 - Internet üzerinden yayınlanmış Türk sitelerine ait veritabanlarından(300.000 user/pass bilgisi)
- Legal Yoldan
 - Arama motorları, wikipedia gibi yerlerden

<http://www.skullsecurity.org/wiki/index.php/Passwords>

İlişkisel Sözcük Üretme(AWLG)

Associative Word List Generator (AWLG) "Searching the Internet to create relevant word lists."

1. Define your search

Type your root words here:

Add

huzeyfe
lifeoverip
test
netsec

Remove

Omit

sunucu guvenligi

Remove


2. Select additional options

- | | |
|---|---|
| <input checked="" type="checkbox"/> Remove common words | <input type="checkbox"/> Numerization (hi->hi1,h2...) |
| <input type="checkbox"/> L33T5P34K | <input checked="" type="checkbox"/> CapiTALIZATION |
| <input checked="" type="checkbox"/> Special chars (\$@) | |

3. Finish

Type this:

c86x3



Generate Word List!

[About AWLG](#) - [News](#) - [Contact Us](#) - [Privacy Policy](#) - [Terms of Use](#) - [Legal Notice](#) - [Examples](#)

İlişkisel Sözcük Üretme(AWLG) -II

Associative Word List Generator (AWLG)

"Searching the Internet to create relevant word lists."

Your word list has been completed!

Finished on Sat Jul 04 13:46:25 GMT 2009

[Download](#)

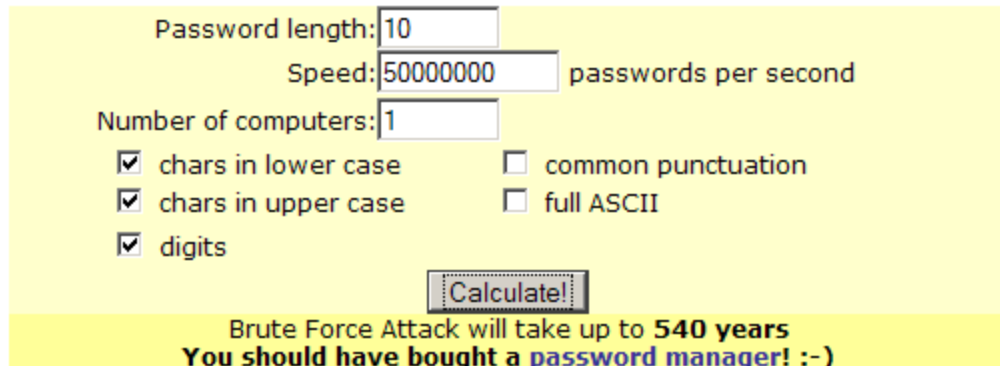
Problems viewing the text file in Notepad in Windows? Use

[Click here to start a new session](#)

language
_qacct
p-18-mFEk4J448M
quantserve
st_go
1427602
wpcom
user_id
subd
ex_go
crypt
addLoadEvent
linktracker_init
Complexity
Enemy
Dosyalarina
Aktif
Izleme
inove
Life
Over
Hakk??mda
Egitimler
NetSec
Listesi
Yaz??lar??m
Monitoring

Brute Force Ataklar

- Belirli bir aralıktaki tüm olasılıkların denenmesi
- Çok başarılı bir atak türü değildir
- Brute force yerine rainbowtable atakları tercih edilmeli.



A screenshot of a web-based calculator for estimating the time required for a brute force password attack. The interface is set against a light yellow background. It includes input fields for 'Password length' (set to 10), 'Speed' (set to 50000000 passwords per second), and 'Number of computers' (set to 1). Below these are checkboxes for character sets: 'chars in lower case', 'chars in upper case', and 'digits' are all checked, while 'common punctuation' and 'full ASCII' are unchecked. A 'Calculate!' button is positioned below the checkboxes. At the bottom, a text box displays the result: 'Brute Force Attack will take up to 540 years' and a warning: 'You should have bought a password manager! :-)'

Password length: 10
Speed: 50000000 passwords per second
Number of computers: 1

☒ chars in lower case ☐ common punctuation
☒ chars in upper case ☐ full ASCII
☒ digits

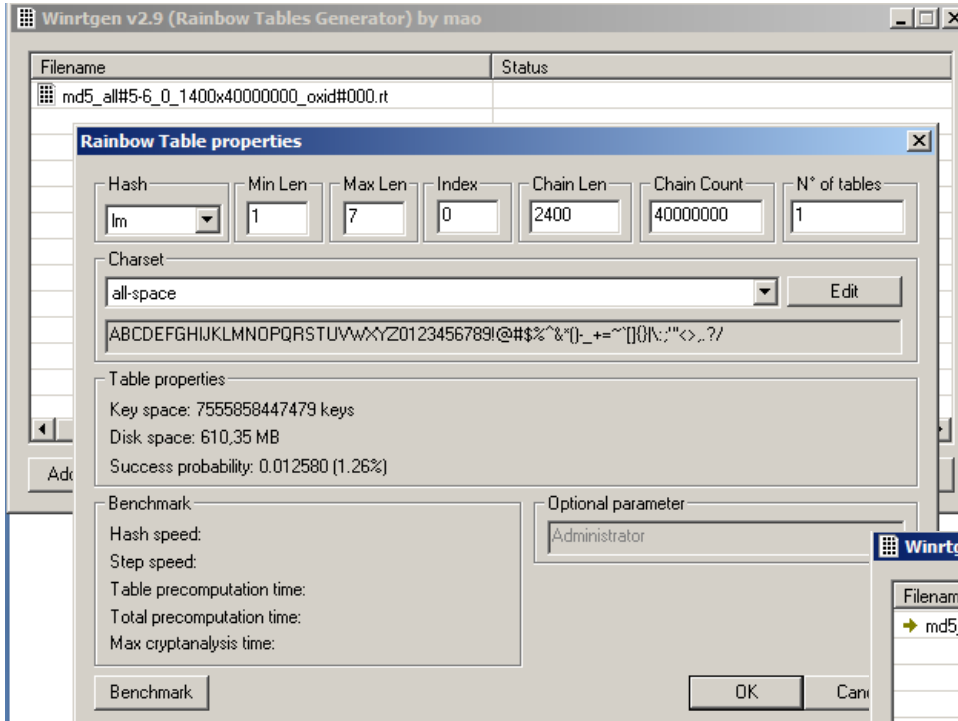
Calculate!

Brute Force Attack will take up to **540 years**
You should have bought a **password manager! :-)**

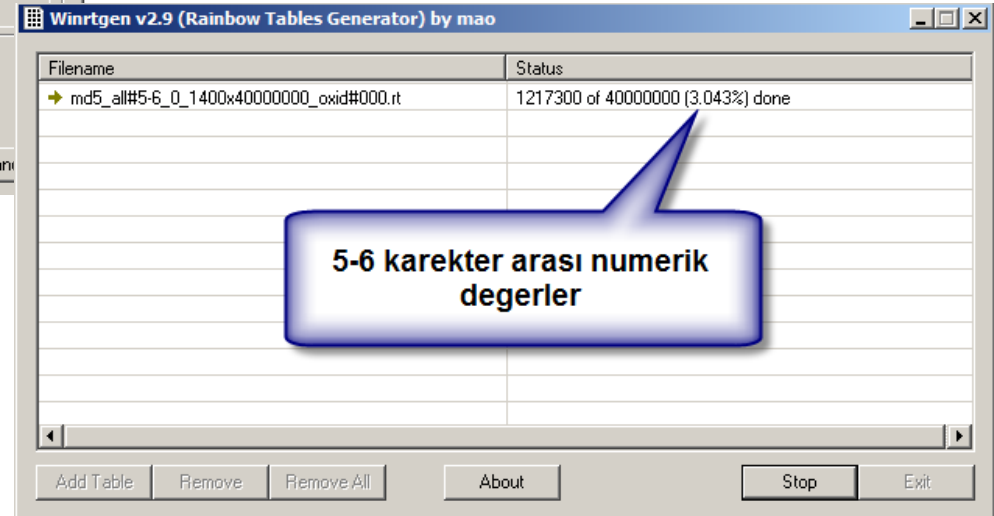
Rainbow Table Atakları

- Pre computed hash mantığı
- Bazı parolalar hash olarak yakalanabilir
 - /etc/shadow, Windows parolaları vs
- Bu tip offline ataklarda yapılacak klasik işlem
- Sözlük saldırısı için
 - İlk sözcüğü al
 - Md5/sha1 hesapla
 - Parola olarak dene, yanlışsa bir sonrakine geç
- Bunun yerine önceden hash değerleri alınmış sözlükler ya da tüm olasılık değerleri kullanılabilir.

Rainbow Tablosu Oluřturma



WinRtGen ile
istenilen türde RT
oluřturulabilir



Rainbow Tablosu Oluşturma Süreleri

charset	[ABCDEFGHIJKLMNOPQRSTUVWXYZ]
keyspace	8353082582
table size	610 MB
success probability	0.9990

charset	[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
keyspace	80603140212
table size	3 GB
success probability	0.9904

charset	[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#\$%^&*()-_+=]
keyspace	915358891407 ($2^{39.7}$)
table size	24 GB
success probability	0.99909

charset	[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#\$%^&*()-_+=~`[]{} .;'<>.,?/]
keyspace	7555858447479 ($2^{42.8}$)
table size	64 GB
success probability	0.999

Laptop üzerinde Ortalama 42 Yıl

Google Üzerinden Parola Kırma

<http://md5.rednoize.com/>



md50;

[Ads by Google](#) [MD5](#) [How to MD5](#) [RSA Encryption](#) [AES Encryption](#)

34819d7beeabb9260a5c854bc85b3e44

MD5 SHA1

mypassword

Md5 Kırma Siteleri

- Hazır rainbowtable içerirler
- Manuel işlem yapmadan önce hash'i bu sitelerde denemeden fayda var.
- Salted hash kullanımı işe yaramaz!

www.rednoize.com

www.md5oogle.com

www.hashmash.com

www.gdataonline.com

www.md5decryption.com

www.md5decrypter.com

www.md5decrypter.co.uk

www.macrosoftware.ro

www.md5-db.com

<http://www.milw0rm.com/cracker/insert.php>

<http://www.plain-text.info>

Parola Tahmini

- Parola tahmini yapılabilmesi için öncelikle Kullanıcı Adı bilgisine ulaşılmalıdır.
- Web uygulamalarında sık görülen durum



The image shows a WordPress login form with the following elements:

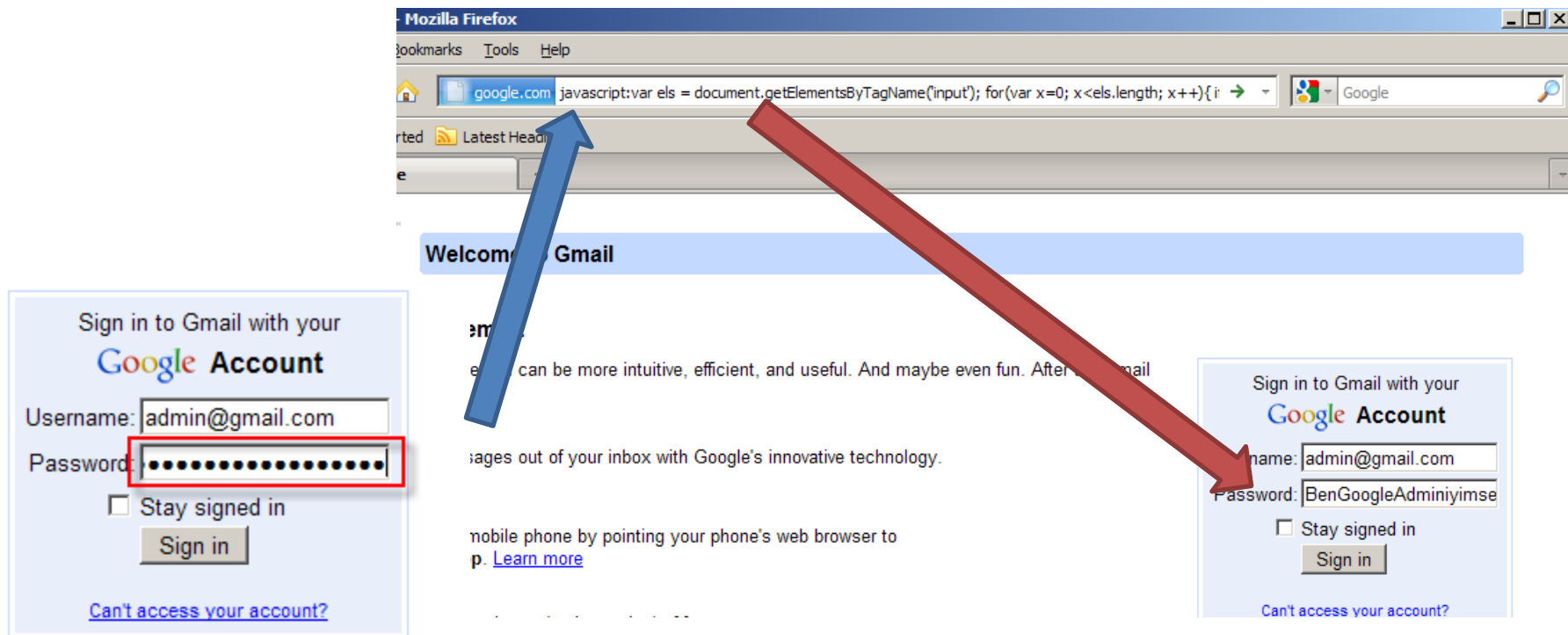
- WordPress logo and text at the top.
- A red-bordered error message box: **ERROR: Incorrect password.**
- A Username input field containing the text **admin**.
- A Password input field with a masked password (dots).
- A ☐ Remember Me checkbox.
- A blue Log In button.
- A [Lost your password?](#) link at the bottom.



The image shows a WordPress login form with the following elements:

- WordPress logo and text at the top.
- A red-bordered error message box: **ERROR: Invalid username.**
- A Username input field containing the text **netsec**.
- A Password input field.
- A ☐ Remember Me checkbox.
- A blue Log In button.
- A [Lost your password?](#) link at the bottom.

Browserdaki Gizli Karakterleri Görüntüleme



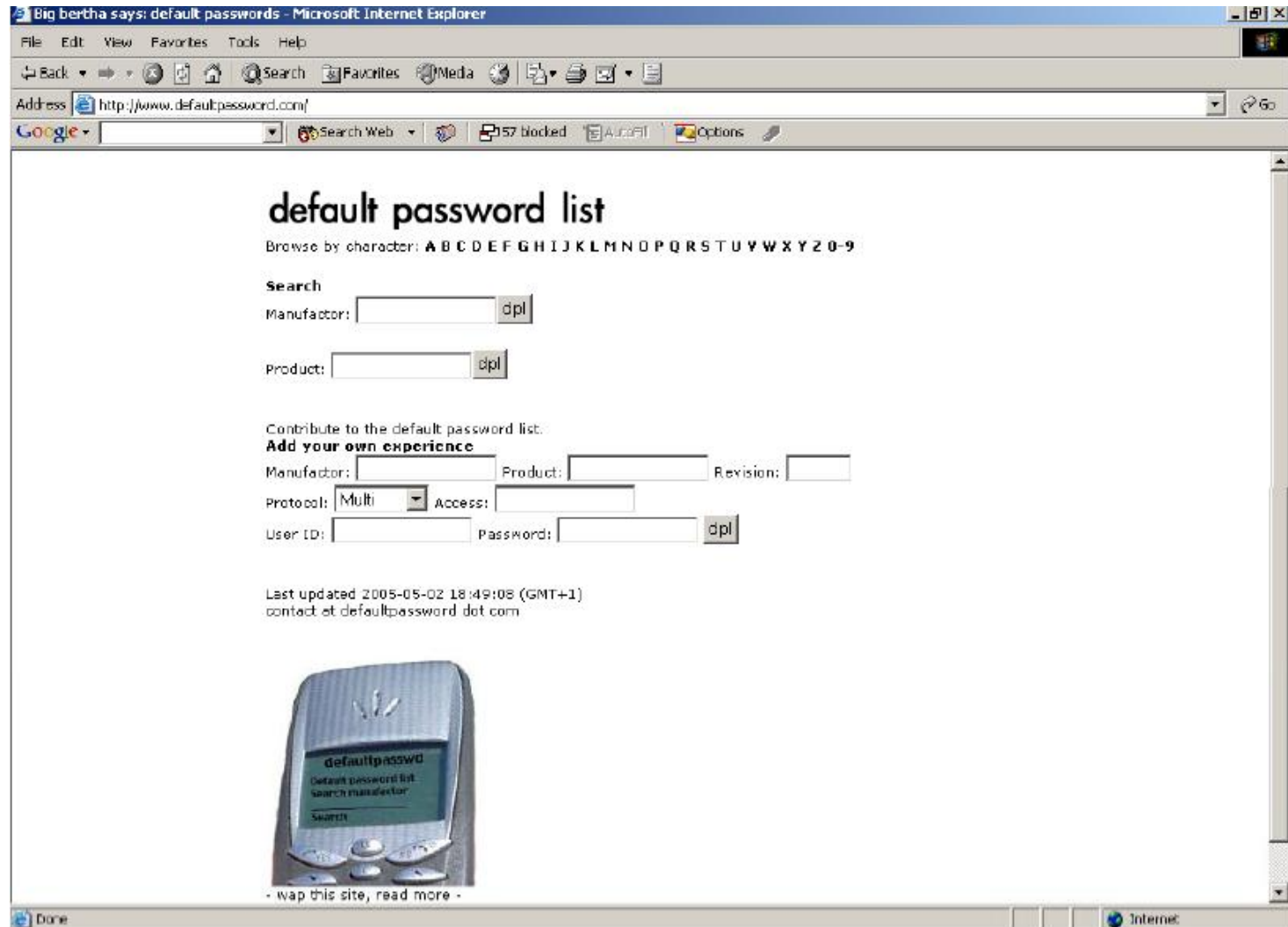
```
javascript:var els = document.getElementsByTagName('input'); for(var x=0; x<els.length; x++){ if(els[x].type.toLowerCase() == 'password' ){ var test = els[x].type = 'text';}}
```

Internet Üzerinde Top 500 Parola

NO	Top 1-100	Top 101-200	Top 201-300	Top 301-400	Top 401-500
1	123456	porsche	firebird	prince	rosebud
2	password	guitar	butter	beach	jaguar
3	12345678	chelsea	united	amateur	great
4	1234	black	turtle	7777777	cool
5	pussy	diamond	steelers	muffin	cooper
6	12345	nascar	tiffany	redsox	1313
7	dragon	jackson	zxcvbn	star	scorpio
8	qwerty	cameron	tomcat	testing	mountain
9	696969	654321	golf	shannon	madison
10	mustang	<u>computer</u>	bond007	murphy	987654
11	letmein	amanda	bear	frank	brazil
12	baseball	wizard	tiger	hannah	lauren
13	master	xxxxxxxx	doctor	dave	japan

<http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time>

Default Parolaların Denenmesi



Varsayılan Router Parolaları

Default Router Passwords - The internet's most comprehensive router password database - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://routerpasswords.com/index.asp

Most Visited Getting Started Latest Headlines

Default Router Passwords - The inte...

ROUTERPASSWORDS

NEW!! Visit the sister [Receiver Passwords](#) site. The worlds Largest Receiver Passwords Database !!

[Eurovox EX1000](#) Only £72.99 | [Eurovox EX1100](#) - Only £79.99
Special: [R4 Card](#) For Nintendo DS -with Kingston 2GB Memory Card £14.99 Next Day Delivery!

Welcome to the internet's most comprehensive **Default router password database 2010**. This is the internet's most complete default router password database available. Simply select the *Router Make* from the dropdown list and click the *Find Password* button.

This database is constantly updated with passwords from visitors like you!! If you know a password that's not listed here, please use the [form](#) to submit it. Remember, this is the worlds largest Router Password database and your help is needed to keep it that way.

If you cant find the make/model you are looking for or would like to [add your a new password](#) to the list, [click here](#).

Select the router manufacturer to find all passwords and models for that router:

Router Make

Vendor	Model	Protocol	Username	Password
3COM	COREBUILDER Rev. 7000/6000/3500/2500	TELNET	debug	synnet
3COM	COREBUILDER Rev. 7000/6000/3500/2500	TELNET	tech	tech
3COM	HIPERARC Rev. V4.1.X	TELNET	adm	(none)
3COM	LANPLEX Rev. 2500	TELNET	debug	synnet
3COM	LANPLEX Rev. 2500	TELNET	tech	tech
3COM	LINKSWITCH Rev. 2000/2700	TELNET	tech	tech
3COM	NETRI III DEF	SNMP		ANYCOM

Twitter Default Parolalar

- Twitter kullanıcı güvenliğini üst düzeye çıkarma amaçlı olarak sık kullanılan parolaların kullanılmasını engellemeye başladı

Kullanıcılara hizmet veren tüm servislerde benzeri önlemler alınmalıdır.

370 banned Twitter passwords

December 27th, 2009 by Dev Team in News

If you look at the source code — on the sign up page — and do a simple search for 'twtr.BANNED_PASSWORDS' you can find all 370 passwords that you can't use. Hit more to see the passwords.

```
twtr.BANNED_PASSWORDS = ["111111", "1111111", "112233",  
"121212", "123123", "123456", "1234567", "12345678", "131313",  
"232323", "654321", "666666", "696969", "777777", "7777777",  
"8675309", "987654", "aaaaa", "abc123", "abc123", "abcdef", "abgrtyu",  
"access", "access14", "action", "albert", "alexis", "amanda", "amateur",  
"andrea", "andrew", "angela", "angels", "animal", "anthony", "apollo",  
"apples", "arsenal", "arthur", "asdfgh", "asdfgh", "ashley", "asshole",  
"august", "austin", "badboy", "bailey", "banana", "barney", "baseball",  
"batman", "beaver", "beavis", "bigcock", "bigdaddy", "bigdick", "bigdog",  
"bigtits", "birdie", "bitches", "biteme", "blazer", "blonde", "blondes",  
"blowjob", "blowme", "bond007", "bonnie", "booboo", "booger",  
"boomer", "boston", "brandon", "brandy", "braves", "brazil", "bronco",  
"broncos", "bulldog", "buster", "butter", "butthead", "calvin", "camaro",  
"cameron", "canada", "captain", "carlos", "carter", "casper", "charles",  
"charlie", "cheese", "chelsea", "chester", "chicago", "chicken", "cocacola",  
"coffee", "college", "compaq", "computer", "cookie", "cooper", "corvette",  
"cowboy", "cowboys", "crystal", "cumming", "cumshot", "dakota",  
"dallas", "daniel", "danielle", "debbie", "dennis", "diablo", "diamond",  
"doctor", "doggie", "dolphin", "dolphins", "donald", "dragon", "dreams",  
"driver", "eagle1", "eagles", "edward", "einstein", "erotic", "extreme",  
"falcon", "fender", "ferrari", "firebird", "fishing", "florida", "flower",  
"flyers", "football", "forever", "freddy", "freedom", "fucked", "fucker",  
"fucking", "fuckme", "fuckyou", "gandalf", "gateway", "gators", "gemini",  
"george", "giants", "ginger", "golden", "golfer", "gordon", "gregory",  
"guitar", "gunner", "hammer", "hannah", "hardcore", "harley", "heather",  
"helpme", "hentai", "hockey", "hooters", "horney", "hotdog", "hunter",  
"hunting", "iceman", "iloveyou", "internet", "iwantu", "jackie", "jackson",  
"jaguar", "jasmine", "jasper", "jennifer", "jeremy", "jessica", "johnny",  
"johnson", "jordan", "joseph", "joshua", "junior", "justin", "killer",
```

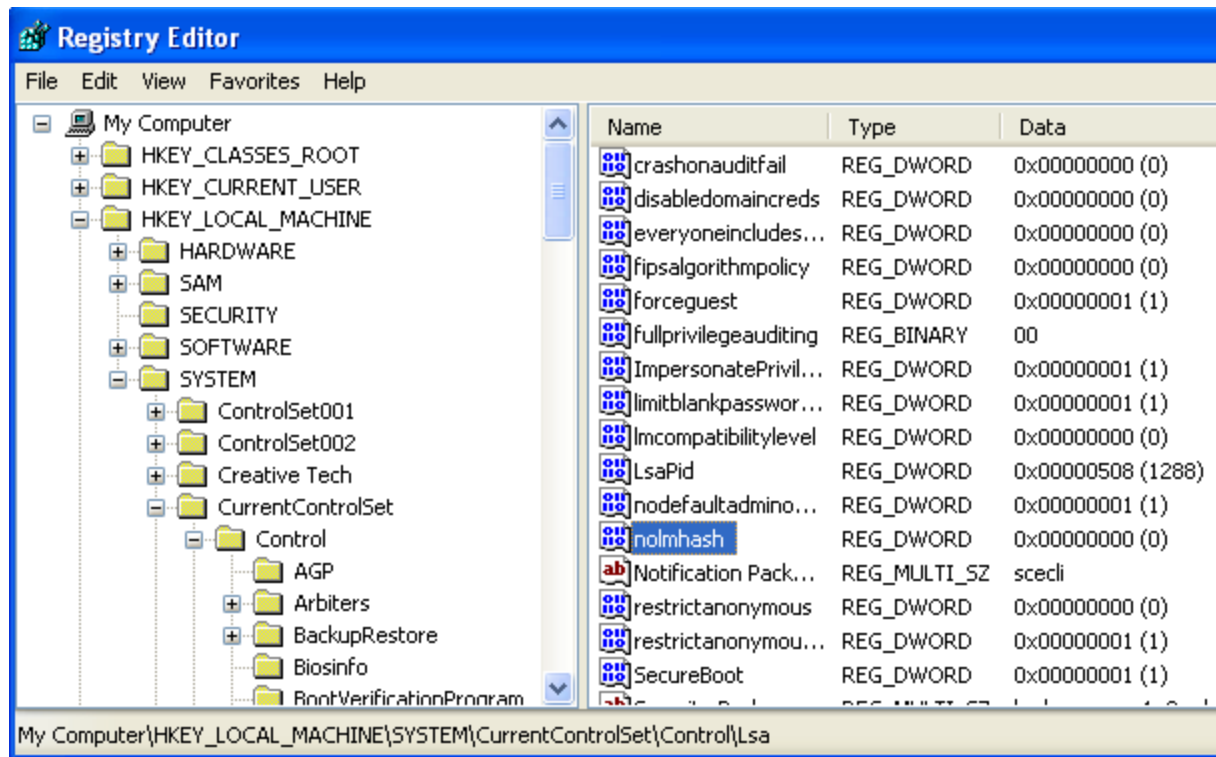
İşletim Sistemleri Parola Güvenliği

- Günümüz modern işletim sistemlerinin hepsi güçlü(!) parola saklama özelliğine sahiptir.

	Windows Systems			Unix-based Systems				
	Windows Vista	Windows Server 2003 Windows XP/ 2000	Windows ME	Red Hat Linux	Ubuntu	Debian	Fedora	Mac OS X 10.4 (2005)
FUNCTION								
DES SymmetriKeys Invertible					X		X	
MD5				X (default)	X (default)	X (default)	X	
SHA							SHA-256/512 (from v.8 is default)	SHA 1 (first time)
LM Hash			X					(second time) ONLY if Windows sharing is enabled
NTLM Hash	X	X						
NT Hash	X (default)							
Salt				X	X	X	X	X

Windows LMHash Disable

- Registry'den...



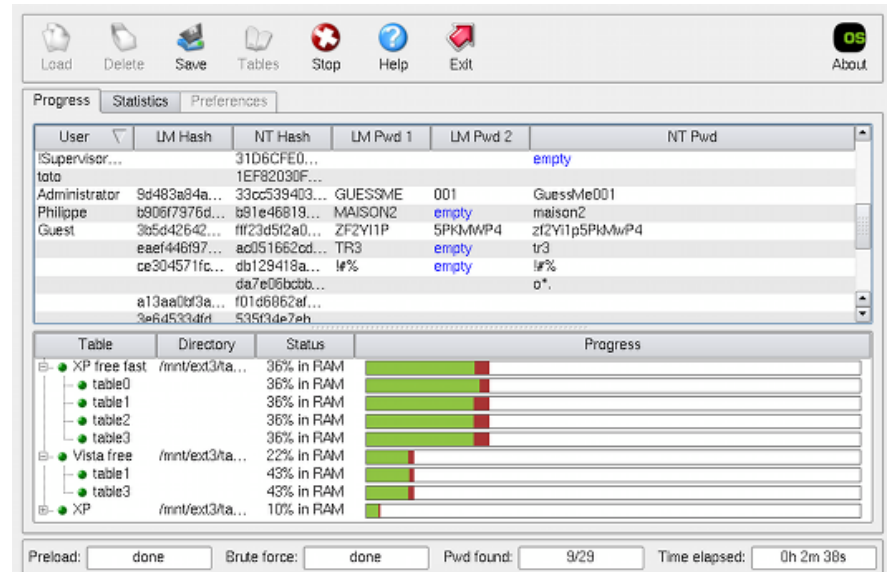
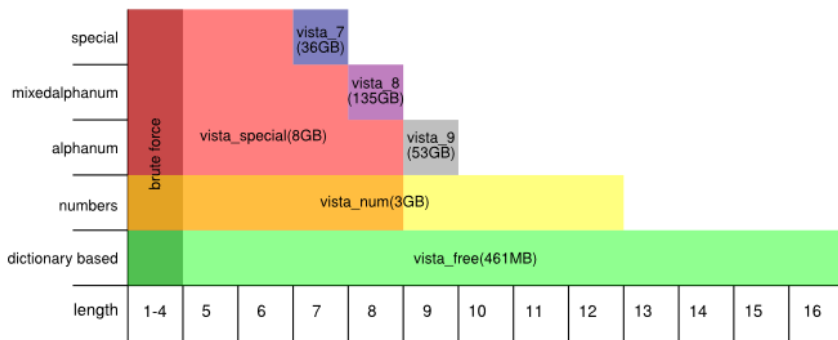
Windows Parola Resetleme

- Amaç varolan parolayı bulma değil, sisteme giriş için yeni parola belirlemedir.
- Araçlar : UBCD4Win, Winntpasswd



Windows Parola Kırma Araçları:OphCrack

- Ücretsiz
- Rainbow tabanlı
- LM ve NTLM hashlerini kırabilir
- Linux/Windows/Mac Os X (Linux Live CD)
- Brute force desteği



LM, NTLM Parola Kirma



Cracker

File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

Cracker

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
Administrator	??????	*		C2265B23734E...	69943C5E63B4D2C104DBBCC15138B72B		LM & NTLM
Guest							LM & NTLM
HelpAssistant							LM & NTLM
Rapsodi							LM & NTLM
root							LM & NTLM
SUPPORT_388945a0							LM & NTLM
__vmware_user__							LM & NTLM
Administrator							LM & NTLM
Guest							LM & NTLM
HelpAssistant							LM & NTLM
Rapsodi							LM & NTLM
root							LM & NTLM
SUPPORT_388945a0							LM & NTLM
__vmware_user__							LM & NTLM

Brute-Force Attack

Charset

Predefined

ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

Custom

Password length

Min 2

Max 7

Start from

12

Keyspace

80603139141

Current password

Key Rate

Time Left

Plaintext of AAD3B435B51404EE is
Plaintext of 4207FD0DF35A59A8 is 12
Attack stopped!
2 of 2 hashes cracked

Linux Sistemler Parola Güvenliği

- UNIX/Linux sistemlerde kullanıcıların parola bilgileri /etc/shadow ya da /etc/master.passwd gibi dosyalarda şifrelenmiş olarak saklanır
- Şifreleme için genelde kullanılan yöntem Md5 olmakla birlikte bazı dağıtımlar SHA256/512 kullanır.
- Parola saldırılarını zorlaştırma için “salt” kullanılır

Parolaların Tuzlanması



Amaç: Önceden hesaplanmış hashlerin kullanımını zorlaştırma

Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d

Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac

Cecil:root:209be1:a483b303c23af34761de02be038fde08

Same
Password

/etc/shadow tipi parola olusturma

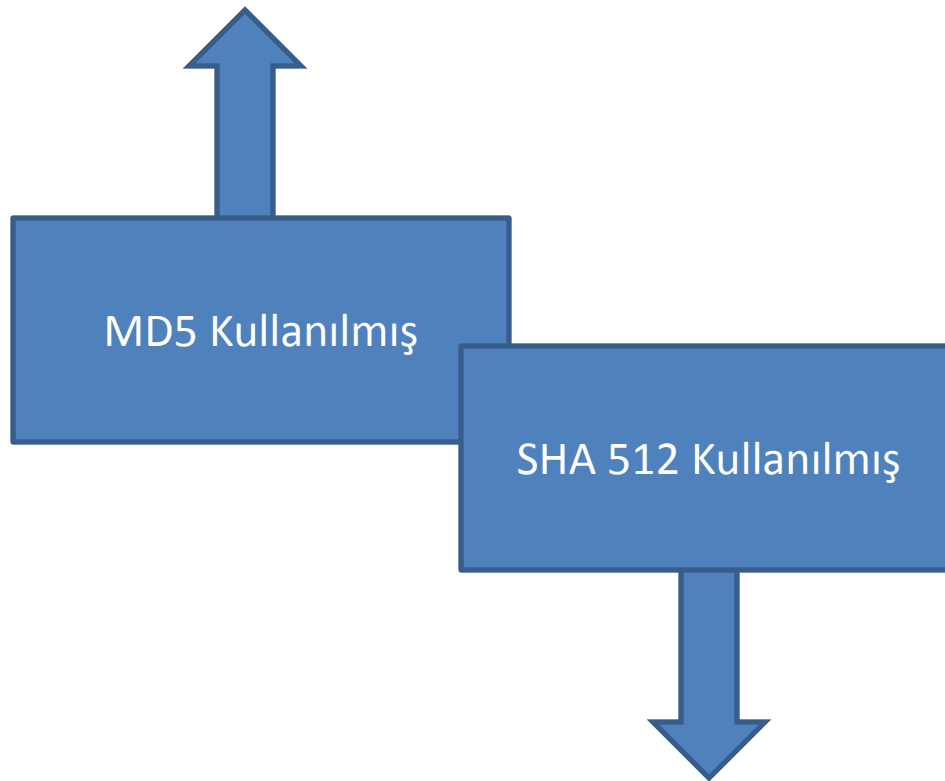
- /etc/shadow dosyasinda sifreli bir sekilde saklanan kullanıcı parolasinin olusturulmasi adimlari;
 - kullanıcı parolayi girer
 - bu parola bir salt değeriyle karıştırılır ve tek yönlü olacak şekilde şifrelenir(Linux sistemler genelde md5 kullanır)
 - bu şifreli değer /etc/shadow dosyasına yazılır.

/etc/shadow tipi parola olusturma-II

- shadow dosyasi içeriği
 - huzeyfe:\$1\$47JagHAu\$6HvvYMo4maDHziTGdB6WT/:13465:0:99999:7::
- kullanıcı isminden sonraki ilk alan şifrelenmiş(?) parolayı gösteriyor.
- Bu alandaki 2. ve 3. \$ işaretleri arasındaki alan salt değeri belirtir.
- # openssl passwd -1 -salt 47JagHAu test123
\$1\$47JagHAu\$6HvvYMo4maDHziTGdB6WT/
-

/etc/shadow Hash Tipleri

huzeyfe:\$1\$47JagHAu\$6HvvYMo4maDHziTGd



huzeyfe:\$6\$47JagHAu\$6HvvYMo4maDHziTGd

Sha512 tipi shadow parolası oluşturma

- Openssl desteği yok
- Mkpaswd kullanılabilir

```
# mkpaswd -m sha-512 -S test
```

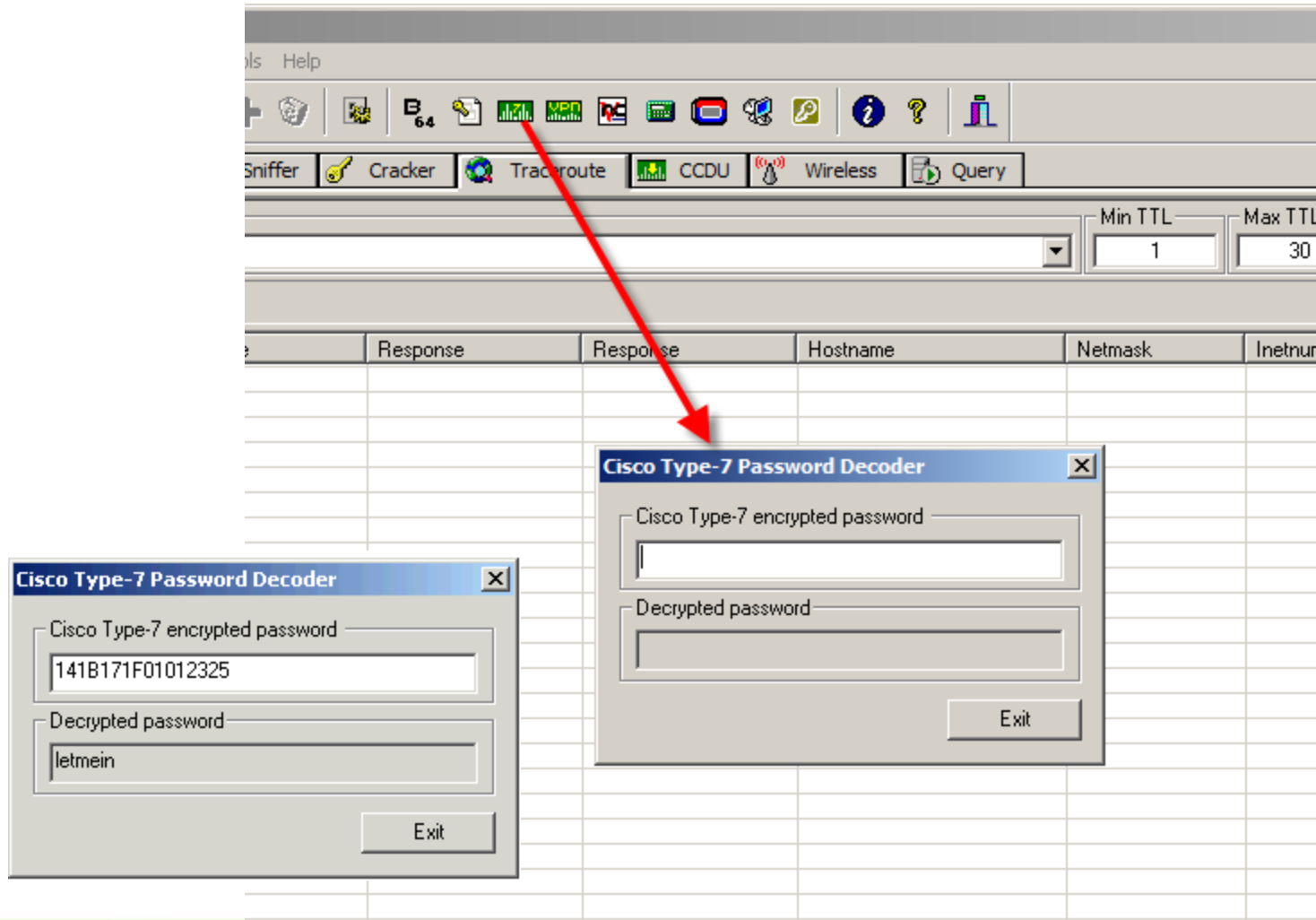
```
$6$hfAI5ZzDnolQ24ib$1bPOt2d2en/IQHn3KB5rYPBM83YaZXsXRfnUziY1hM/41pEEkguyu3jtiVKjoUxEyn2  
qfo6eqrwFguCnA/Xsy/
```

Cisco Parola Güvenliği

- Type 5 ve Type 7 parolaları
- Type7 =encoded bir parola
- Type 5 md5+hash alınmış bir parola



Cisco Parola Güvenliği



Cisco enable parolası



- Cisco enable parolası kaydedilirken Linux sistemlerdekine benzer mantık işler
- Bunun sebebi Cisco IOS'un FreeBSD şifreleme kütüphanesini kullanmasıdır
- Router(config)#enable secret HL_R12
- Router#sh run | include enable secret
5 \$1\$RK5L\$05G045n5XVIENtyo04PBT1
- Router#sh run | include enable secret
- Router#sh run | include password (Cisco Type 7)
- John the ripper kullanarak kırılabilir

Parola Kırma Araçları

- Açık kaynak kodlu ve ticari çeşitli araçlar
- Windows/Linux desteği
- Medusa
- Hydra
- Rtcrack,rtgen, Winrtgen
- Cain&Abel
- Brutessh
- Brutus
- John The Ripper



SSh BruteForce

```
root@home-labs:/pentest/password/brutessh# python brutessh.py -h  
192.168.2.27 -u huzeyfe -d /root/mil-dic.php
```



```
*****
```

```
*SSH Bruteforcer Ver. 0.2      *  
*Coded by Christian Martorella  *  
*Edge-Security Research        *  
*laramies@gmail.com           *
```

```
*****
```

```
HOST: 192.168.2.27 Username: huzeyfe Password file: /root/mil-dic.php
```

```
=====
```

```
Trying password...
```

```
NetseC
```

SSHBruteForce Analizi

- Parola dosyasının uzunluğu 83.000 civarında ve bulunan parola dosyanın sonundadır.

```
# wc -l /root/mil-dic.php
```

```
83310
```

- Bu işlem toplamda 13 dakika sürmüştür. Bu esnada sistem üzerinde SSH servisine dışarıdan bağlanılamaz hale gelir.

SSH BruteForce Saldırı İncelemesi

- Bu esnada sistemin auth loguna bakılırsa yapılan denemeler gözükecektir.

```
root@home-labs:~# tail /var/log/auth.log
```

```
Jul 4 08:52:37 home-labs sshd[11252]: Failed password for huzeyfe from 192.168.2.27  
port 59499 ssh2  
Jul 4 08:52:37 home-labs sshd[11257]: Failed password for huzeyfe from 192.168.2.27  
port 59500 ssh2  
Jul 4 08:52:37 home-labs sshd[11268]: Failed password for huzeyfe from 192.168.2.27  
port 59505 ssh2  
Jul 4 08:52:37 home-labs sshd[11276]: Failed password for huzeyfe from 192.168.2.27  
port 59508 ssh2  
Jul 4 08:52:38 home-labs sshd[11284]: Failed password for huzeyfe from 192.168.2.27  
port 59511 ssh2  
Jul 4 08:52:38 home-labs sshd[11296]: Failed password for huzeyfe from 192.168.2.27  
port 59514 ssh2  
Jul 4 08:52:38 home-labs sshd[11289]: Failed password for huzeyfe from 192.168.2.27  
port 59512 ssh2  
Jul 4 08:52:38 home-labs sshd[11300]: Failed password for huzeyfe from 192.168.2.27  
port 59515 ssh2  
Jul 4 08:52:38 home-labs sshd[11304]: Failed password for huzeyfe from 192.168.2.27  
port 59516 ssh2  
Jul 4 08:52:38 home-labs sshd[11292]: Failed password for huzeyfe from 192.168.2.27  
port 59513 ssh2
```

Medusa ile Parola Kırma saldırıları

- Güncel
- Desteklediği modül sayısı fazla
- Kolay kullanım



Medusa tarafından desteklenen modüller

medusa -d

Medusa v1.4 [<http://www.foofus.net>] (C) JoMo-Kun / Foofus Networks jmk@foofus.net

Available modules in ".":

Available modules in "/usr/lib/medusa/modules":

- + cvs.mod : Brute force module for CVS sessions : version 1.0.0
- + ftp.mod : Brute force module for FTP/FTPS sessions : version 1.3.0
- + http.mod : Brute force module for HTTP : version 1.3.0
- + imap.mod : Brute force module for IMAP sessions : version 1.1.0
- + mssql.mod : Brute force module for MS-SQL sessions : version 1.1.1
- + mysql.mod : Brute force module for MySQL sessions : version 1.2
- + ncp.mod : Brute force module for NCP sessions : version 1.0.0
- + nntp.mod : Brute force module for NNTP sessions : version 0.9
- + pcanywhere.mod : Brute force module for PcAnywhere sessions : version 1.0.2
- + pop3.mod : Brute force module for POP3 sessions : version 1.1.1
- + postgres.mod : Brute force module for PostgreSQL sessions : version 1.0.0
- + rexec.mod : Brute force module for REXEC sessions : version 1.1.1
- + rlogin.mod : Brute force module for RLOGIN sessions : version 1.0.2
- + rsh.mod : Brute force module for RSH sessions : version 1.0.1
- + smbnt.mod : Brute force module for SMB/NTLMv1 sessions : version 1.3.1
- + smtp-auth.mod : Brute force module for SMTP Authentication with TLS : version 0.9.1
- + smtp-vrfy.mod : Brute force module for enumerating accounts via SMTP VRFY : version 0.9.1
- + snmp.mod : Brute force module for SNMP Community Strings : version 1.0.0
- + ssh.mod : Brute force module for SSH v2 sessions : version 1.0.2
- + svn.mod : Brute force module for Subversion sessions : version 1.0.0
- + telnet.mod : Brute force module for telnet sessions : version 1.2.1
- + vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 1.0.0
- + vnc.mod : Brute force module for VNC sessions : version 1.0.1
- + web-form.mod : Brute force module for web forms : version 0.9
- + wrapper.mod : Generic Wrapper Module : version 1.0.1

Yardım Menüsü

medusa -M mysql -q

Medusa v1.4 [<http://www.foofus.net>] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

mysql.mod (1.2) JoMo-Kun <jmk@foofus.net> :: Brute force module for MySQL sessions

Available module options:

PASS:? (PASSWORD*, HASH)

PASSWORD: Use normal password.

HASH: Use a hash rather than a password. (non-SHA1 hashes only)

(*) Default value

Usage examples:

1: Normal boring check...

medusa -M mysql -h somehost -u someuser -p somepassword

2: Using an old-style MySQL hash...

medusa -M mysql -h somehost -U users.txt -p 39b52a209cf03d62 -m PASS:HASH

Mysql Parola Testi



```
# medusa -M mysql -h localhost -u root -P /root/wordlist
Medusa v1.4 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [mysql] Host: 127.0.0.1 (1/1) User: root (1/1) Password: test (1/5)
ACCOUNT CHECK: [mysql] Host: 127.0.0.1 (1/1) User: root (1/1) Password: deneme (2/5)
ACCOUNT CHECK: [mysql] Host: 127.0.0.1 (1/1) User: root (1/1) Password: alibaba (3/5)
ACCOUNT CHECK: [mysql] Host: 127.0.0.1 (1/1) User: root (1/1) Password: toor (4/5)
ACCOUNT FOUND: [mysql] Host: 127.0.0.1 User: root Password: toor [SUCCESS]
```


Brutessh ile SSH parola tahmini



```
# python brutessh.py -h localhost -u root -d /root/wordlist
```

```
*****  
*SSH Bruteforcer Ver. 0.2      *  
*Coded by Christian Martorella *  
*Edge-Security Research       *  
*laramies@gmail.com           *  
*****
```

```
HOST: localhost Username: root Password file: /root/wordlist
```

```
=====
```

Trying password...

```
Auth OK ---> Password Found: toor  
12334
```

```
Times --> Init: 0.04 End: 0.55
```

```
Alibaba
```

Basic Authentication Testi

- **#medusa -M http -m USER-AGENT:"Firefox-Explorer-99.1" -m DIR:/test -m AUTH:BASIC -h 10.10.10.1 -u bga -P bga-wordlist22**
- /test dizini aşağıdaki gibi .htaccess korumasına sahiptir.

```
AuthUserFile /etc/.htpasswd-1
AuthGroupFile /dev/null
AuthName "Giris Yasak!"
AuthType Basic
```

```
<Limit GET POST>
require valid-user
</Limit>
```

Ağ servislerine Parola Denetimi

- Depant ((DE)fault (PA)ssword (N)etwork (T)ool).
- Ağ üzerindeki servislere nmap ve hydra kullanarak bilinen kullanıcı adı/parola ikililerini deneyerek rapor çıkarır.

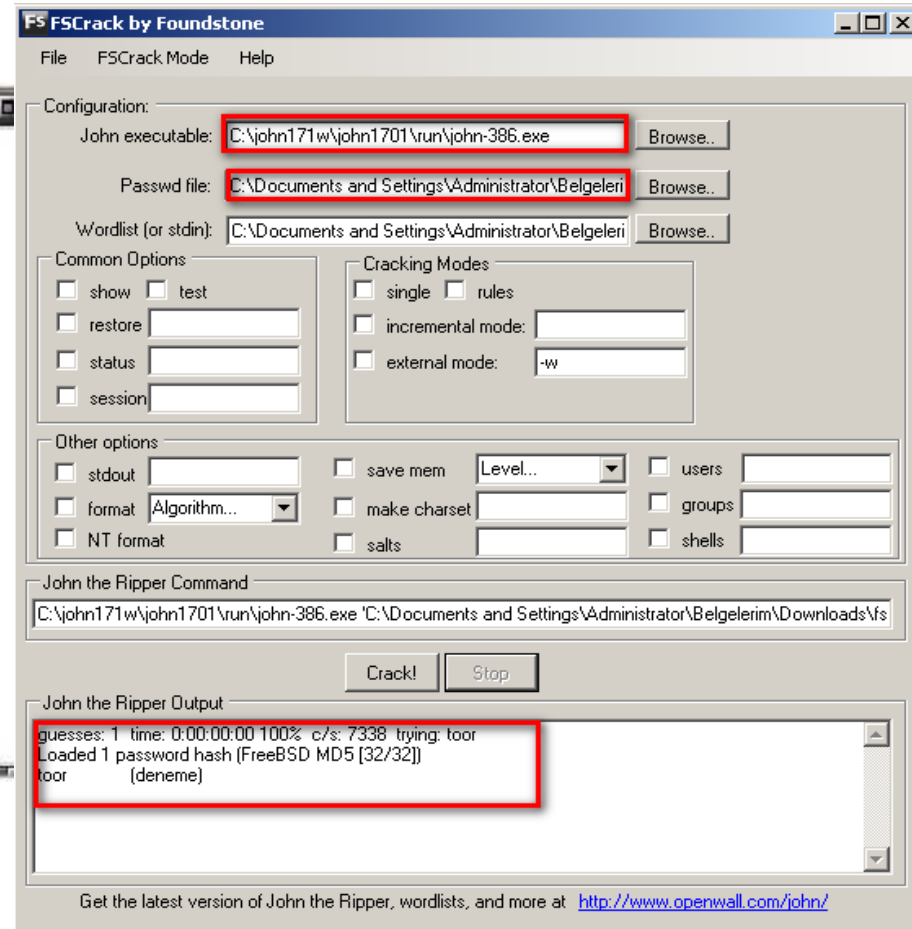
```
$ depant -c ./dpl -U ./user.txt -P ./pass.txt -H 127.0.0.1/30

--[[ Depant v0.1a ]]=--
--[[ Midnight Research Labs ]]=--

[*] Phase 2 scanning enabled
[*] Starting phase 1 nmap scan of [2] host(s)
[*] Adding host [127.0.0.1] port [22] to list of services to test
[*] Found [1] thing(s) to check for default passwords
[*] Starting phase 1 hydra scans
[*] Checking for default passwords on host [127.0.0.1] port [22]
[*] Fastest service to run second phase on is [127.0.0.1] port [22]
[*] We did not find results in phase one... going to second phase
[*] Starting phase 2
[*] Checking for default passwords on host [127.0.0.1] port [22]
[!!!] Found user [testuser] with pass [YourPasswordSucks] on [127.0.0.1] service/port [22]
[!!!] We found logins on [1] hosts
[*] Total runtime was [34] seconds
[*] Finished.
```

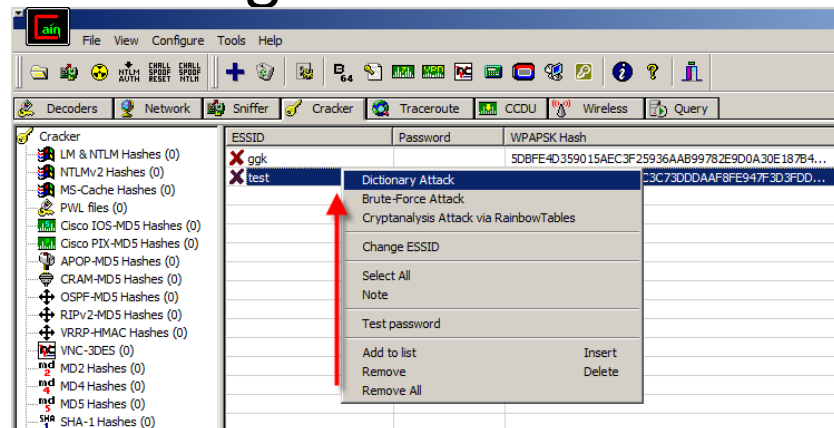
John The Ripper

```
root@fred:/home/tools/john-1.6/run
[root@fred tools]# cd /home/tools/john-1.6/run
[root@fred run]# cp /etc/passwd ./passwd.bak
[root@fred run]# cp /etc/shadow ./shadow.bak
[root@fred run]# ./unshadow
Usage: ./unshadow PASSWORD-FILE SHADOW-FILE
[root@fred run]# ./unshadow passwd.bak shadow.bak > crackthis.txt
[root@fred run]# ./john crackthis.txt
Loaded 4 passwords with 4 different salts (FreeBSD MD5 [32/32])
htimshplar      (ralph)
guesses: 1 time: 0:00:00:19 6% (2) c/s: 1702 trying: bobcats
guesses: 1 time: 0:00:00:22 8% (2) c/s: 1702 trying: christia1
guesses: 1 time: 0:00:00:24 9% (2) c/s: 1702 trying: Missy1
guesses: 1 time: 0:00:00:26 10% (2) c/s: 1703 trying: Start1
guesses: 1 time: 0:00:00:28 11% (2) c/s: 1703 trying: mozartmozart
```

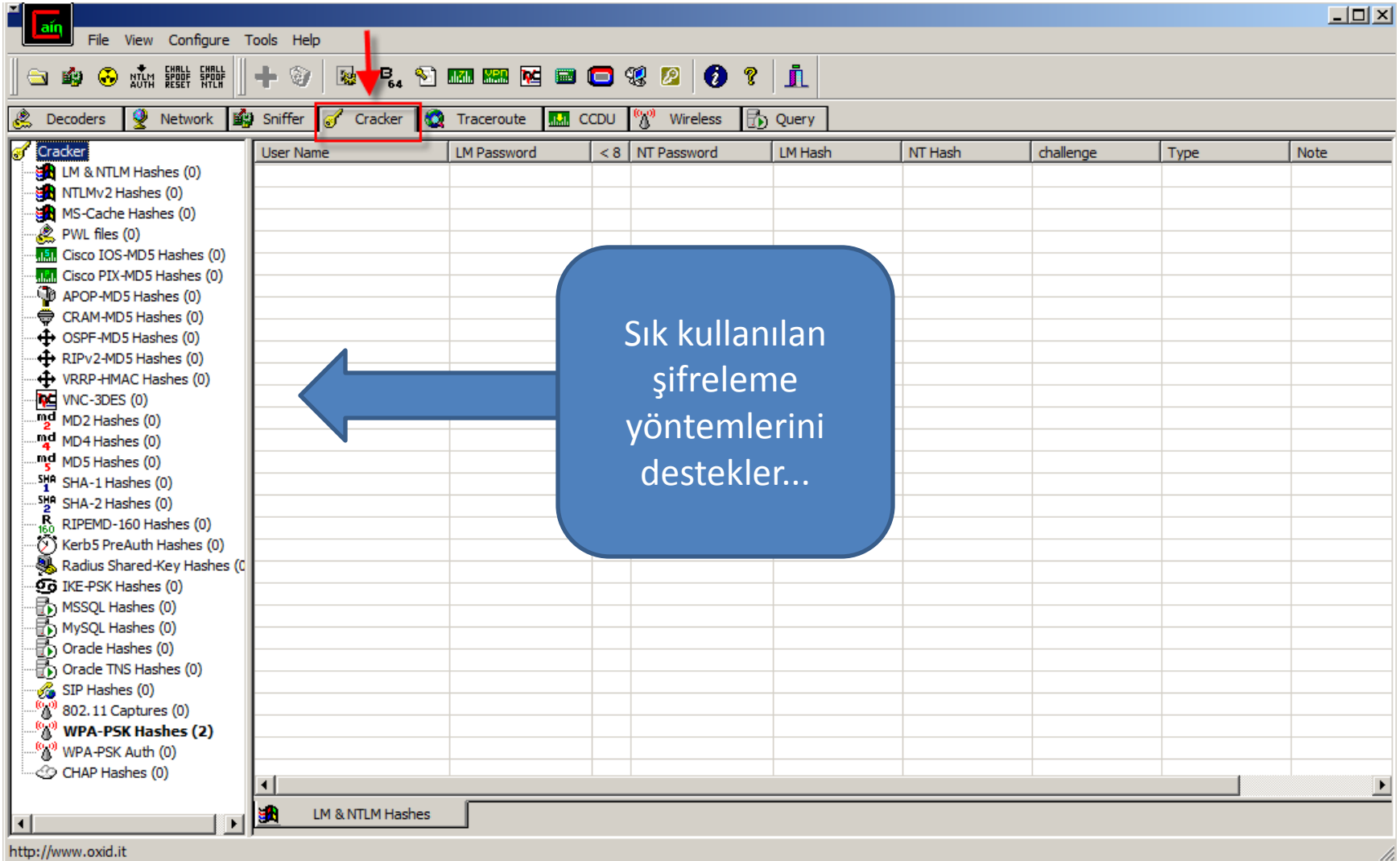


Cain & Abel

- Windows tabanlı parola kırma ve network güvenliği test aracı
- Parola Güvenliği Testleri için;
 - Rainbow table desteği
 - Dictionary Password crack desteği
 - Bruteforce
 - Kriptoanaliz
 - WEP/WPA Crack desteği

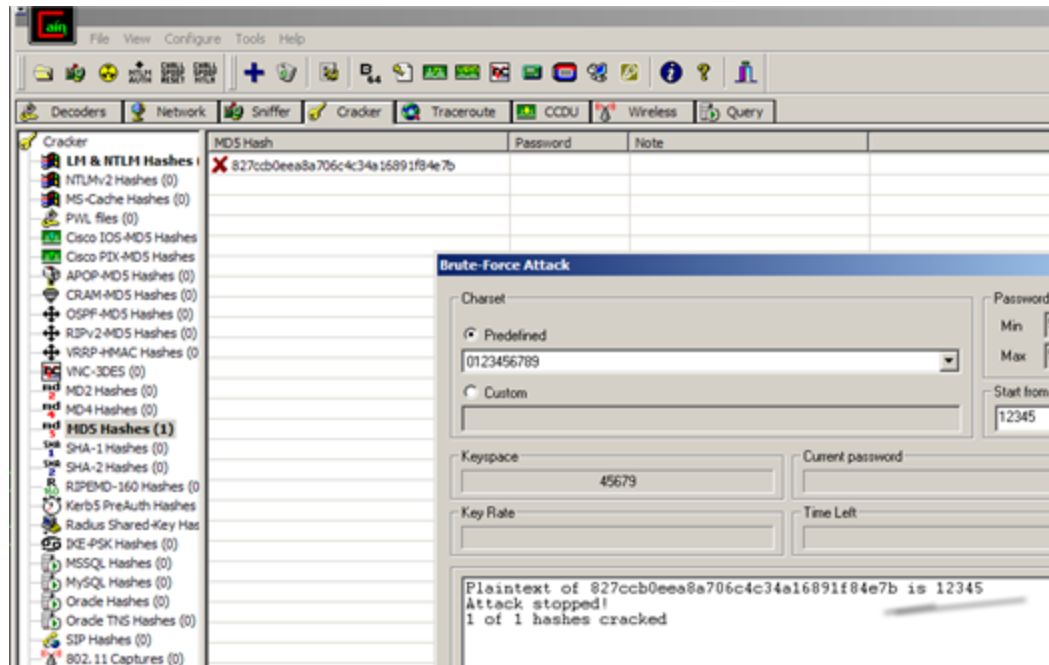


Cain Tarafından Desteklenen Şifreleme Tipleri



Cain tarafından desteklenen hash algoritmaları

- MD2, MD4, MD5, SHA1, SHA2 (256 bit), SHA2 (384 bit), SHA2 (512 bit), RIPEMD160.



Cain&Abel Parola Kırma Yöntemleri

Cracker	User Name	LM Pas...	NT Pas...	LM Hash	NT Hash	Type
LM & NTLM Hashes (6)	Administrator					LM & NTLM
NTLMv2 Hashes (0)	ASPNET			E2A6F179F813186428D4ED3C42AB0586	E8192C0D7D61464C1E7FF0BE613D691B	LM & NTLM
MS-Cache Hashes (0)	Guest	* empty *	* empty *	NO PASSWORD*****	NO PASSWORD*****	
PWL files (0)	HelpAssistant			5FF9DC1C55A7866C8E9D3B7AE61EE185	B7D585D0CF615031FFD443EB40909DE3	LM & NTLM
Cisco IOS-MD5 Hashes (0)	korhan					LM & NTLM
Cisco PIX-MD5 Hashes (0)	SUPPORT_388945a0	* empty *		NO PASSWORD*****	BCE7F30E2A95D8972A880582B9097D43	NTLM
APOP-MD5 Hashes (0)						
CRAM-MD5 Hashes (0)						

Dictionary Attack

Brute-Force Attack

Cryptanalysis Attack

Rainbowcrack-Online

ActiveSync

Select All

Test password

Add to list

Remove

Remove All

Export

LM Hashes

LM Hashes + challenge

NTLM Hashes

NTLM Hashes + challenge

NTLM Session Security Hashes

Dictionary Attack

Brute-Force Attack

Cryptanalysis Attack

Rainbowcrack-Online

ActiveSync

Select All

Test password

Add to list

Remove

Remove All

Export

LM Hashes

LM Hashes + challenge

NTLM Hashes

NTLM Hashes + challenge

NTLM Session Security Hashes

Dictionary Attack

Brute-Force Attack

Cryptanalysis Attack

Rainbowcrack-Online

ActiveSync

Select All

Test password

Add to list

Remove

Remove All

Export

3EF5B908CFD87C7788206D79311F09A8

6A34DFBBA0E9FF851DE59C376277

NO PASSWORD*****

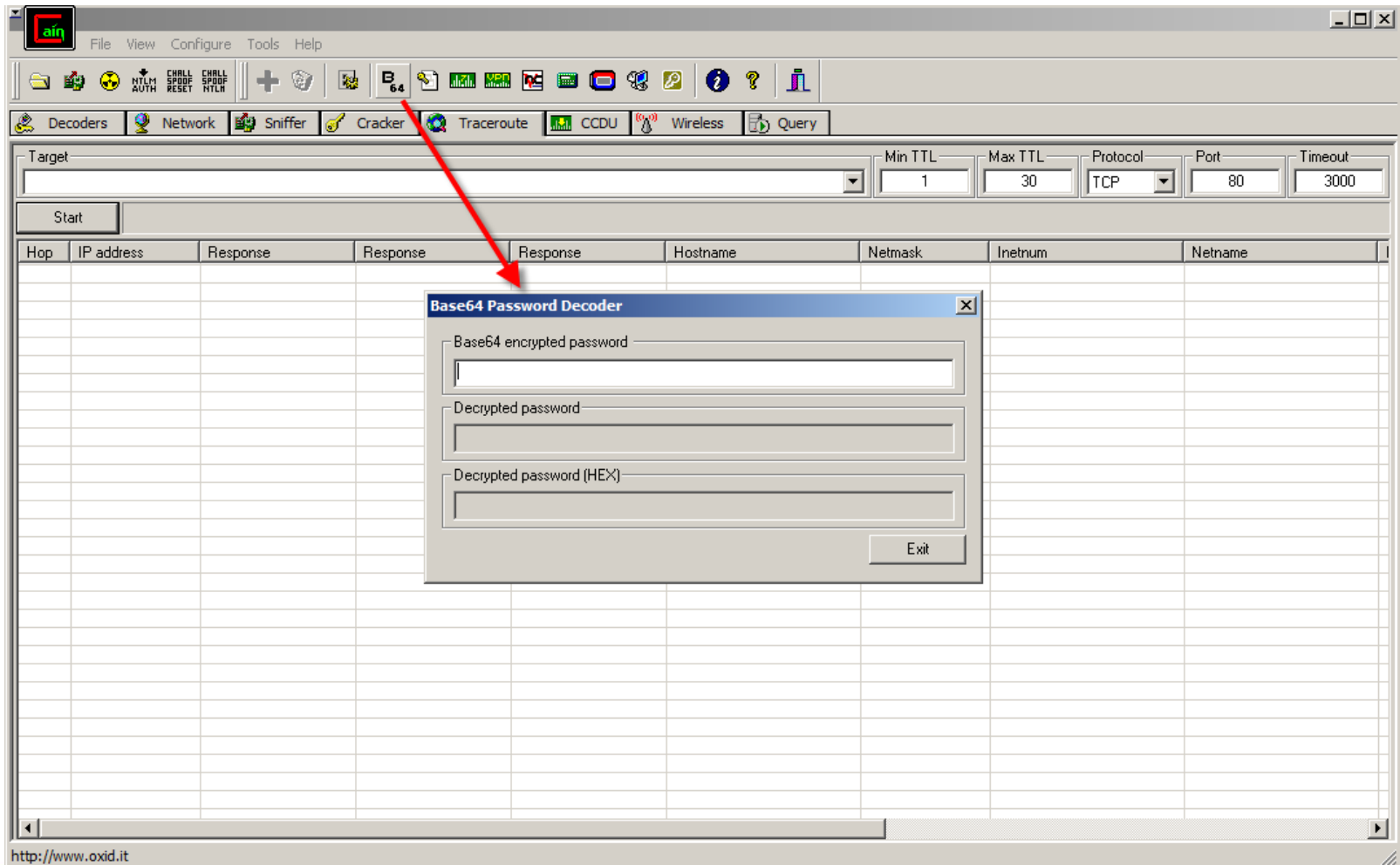
BCE7F30E2A95D8972A880582B909

via RainbowTables (OphCrack)

via RainbowTables (RainbowCrack)

via FastLM RainbowTables (Winrtgen)

Base64 Encode/Decode



Keylogger Kavramı

- Nedir ?
- Nasıl çalışır ?
- Çeşitleri ?
 - Yazılım tabalı.
 - Donanım tabanlı.
- Engelleme yöntemleri ?
- Antilogger yazılımları



Yazılım Tabanlı Keylogger' lar

- Nedir ?
- Nasıl çalışır ?
- Hangi bilgilere erişebilir
 - Tüm klavye girişlerini kaydetme.
 - Ekran görüntüsü yakalama.
 - Alınan bilgileri mail yolu ile sahibine iletebilme.
- Nasıl tespit edilir ?

Donanım Tabanlı Keylogger' lar

- Nedir ?
- Nasıl çalışır ?
- Hangi bilgilere erişebilir
 - Tüm klavye girişlerini kaydetme.
 - Ekran görüntüsü yakalama.
 - Alınan bilgileri mail yolu ile sahibine iletebilme.

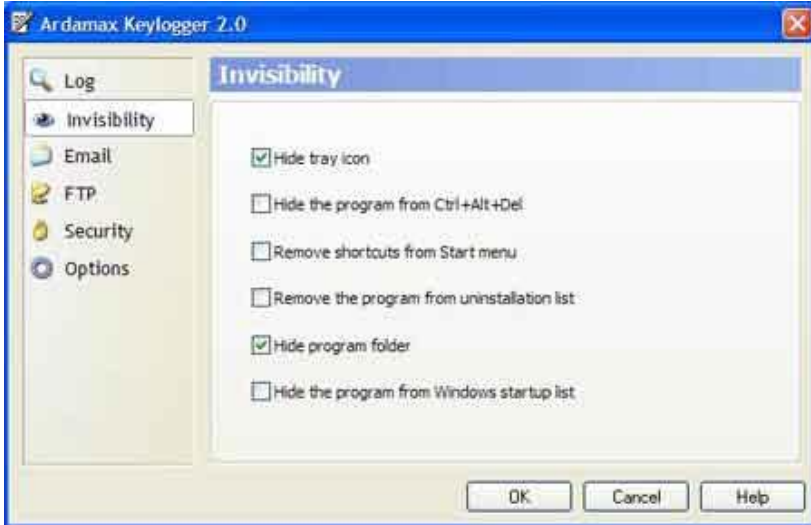
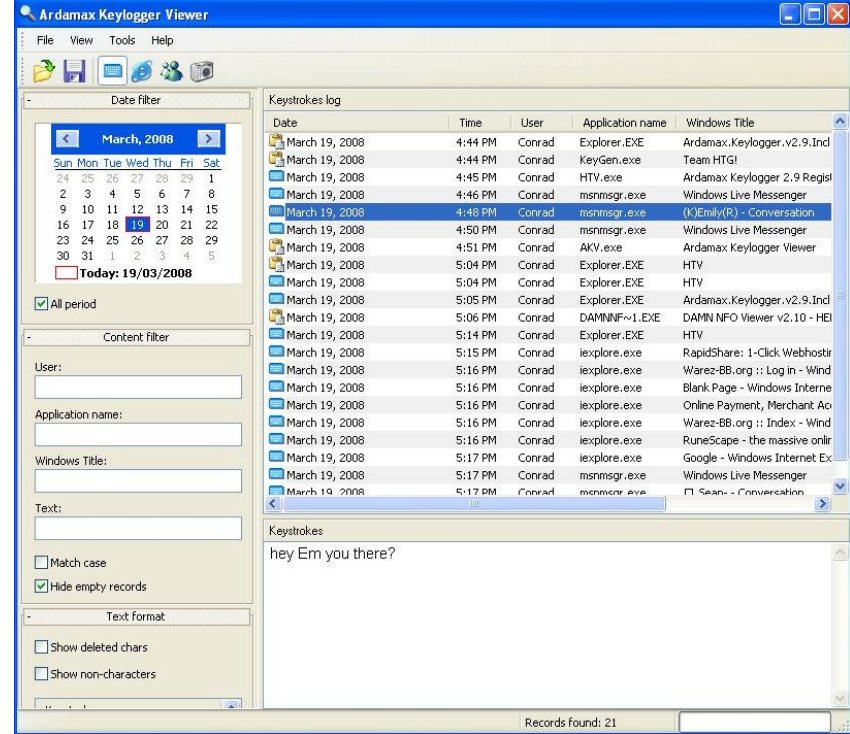
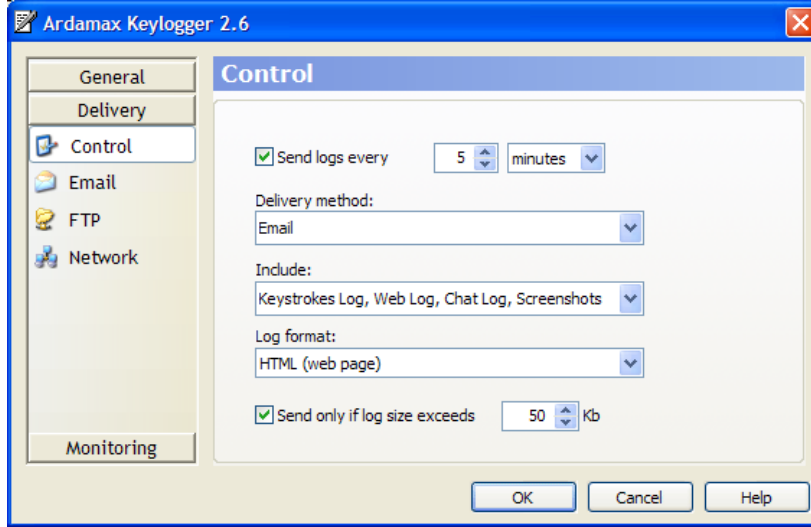
Keylogger' lara Karşı Alınacak Önlemler

- Etkin içerik ve sınır güvenliği.
- Etkin client güvenlik politikaları.
 - Antivirus yazılımları
 - Uygula ve İşletim sistemi patch yönetimi.
- Yerel ağ güvenliği
 - Anormal trafik tiplerinin tespiti.
 - Yabancı kullanıcıların ve kurum çalışanların bir güvenli şekilde yerel ağa dahil edilmesi ve erişimi (NAC çözümleri)

Bilinen Keylogger 'lar

- Yazılım Tabanlı
 - Ardamax
 - Perfect Keylogger
 - KeyGrab
- Donanım Tabanlı
 - PS/2 Keylogger
 - USB Keylogger
 - Wi-Fi Keylogger
 - Module Keylogger
 - <http://www.keelog.com>

Keylogger Ekran Görüntüleri



Donanım Tabanlı Keylogger' lar



Fiziksel Zafiyetler.

- Kurbanın klavye hareketlerini gözlemlere parola tahmini.
- Alınabilecek önlemler
 - Biometrik kimlik doğrulama sistemleri.
 - Parmak izi tanıma.
 - Retina tanıma.
 - Yüz tanıma sistemleri vs.
 - Kullanıcıları bilgi güvenliği konusunda bilinçlendirme.
 - Vs vs.

