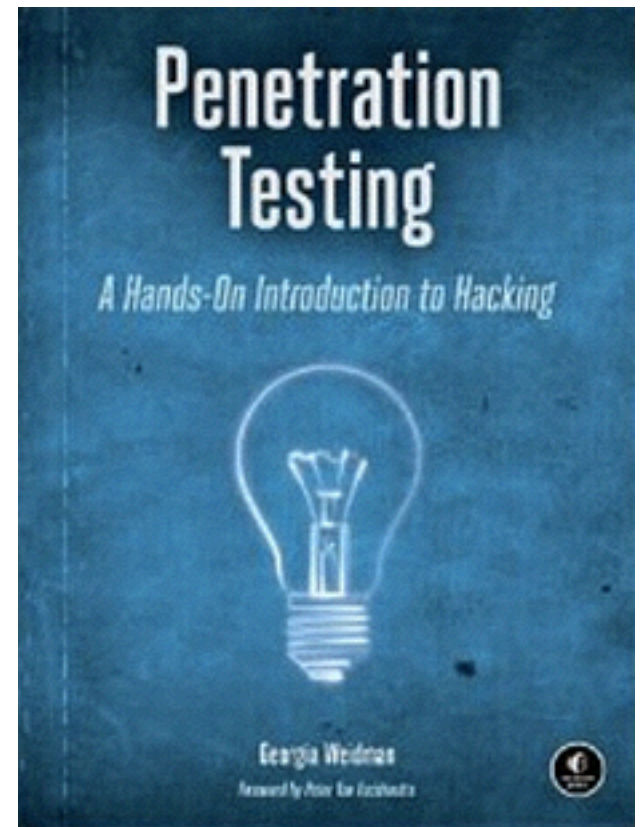


CNIT 124: Advanced Ethical Hacking



Ch 9: Password Attacks

Topics

- Password Management
- Online Password Attacks
- Offline Password Attacks
- Dumping Passwords from RAM

Password Management

Password Alternatives

- Biometrics
- Two-factor authentication
- Digital certificates

iPhone X



Secure
Authentication

Your face is now your password. Face ID is a secure new way to unlock, authenticate, and pay.

Common Password Errors

- Short passwords
- Using dictionary words
- Re-using passwords
 - Attackers know that a stolen password can often be re-used elsewhere

Password Reset

- A weak spot for cloud services, especially free ones

Teen says he hacked CIA director's AOL account

By Philip Messing, Jamie Schram and Bruce Golding

October 18, 2015 | 11:40pm



Online Password Attacks

Multiple Logins

- Scripts try to login with passwords from a list
- Can be blocked by **lockout policies**
 - After five failed logins, must wait an hour
- Brute-forcing is possible
 - Trying every combination of characters
 - Impractical except for very short passwords

Wordlists

- Usernames
 - Look at valid account names, try to deduce the pattern
 - CCSF uses first letter of first name, then last name, then 2 digits, like psmith01
 - Find a list of real usernames, or use a list of common names

Password Lists

- Packetstorm
- For special purposes
- Openwall has more general ones, but they cost money
 - Link Ch 9d



The screenshot shows a web browser window with the address bar displaying <https://packetstormsecurity.com/Crackers/wordlists>. The page content is as follows:

- asteroid.gz**
Word list created from asteroid names. (3459 words)
tags | [cracker](#)
MD5 | 90fcd27dd54dc0ce16cfa59346b9d845
- kj-bible.gz**
Word list created from the King James Bible. (13044 words)
tags | [cracker](#)
MD5 | 8298184786e8236796ea65d79a58068c
- koran.gz**
Word list created from the Koran. (5356 words)
tags | [cracker](#)
MD5 | 7dc6c2a785583eb3c1ba8baced5e8d8f

Targeting Wordlists

- Use information about the targeted person
- Such as a Facebook page
- Generate passwords from clues
 - *TaylorSwift13!*

Cewl

```
root@kali:/usr/share/wordlists# cewl --help
CeWL 5.1 Robin Wood (robin@digi.ninja) (http://digi.ninja)

Usage: cewl [OPTION] ... URL
  --help, -h: show help
  --keep, -k: keep the downloaded file
  --depth x, -d x: depth to spider to, default 2
  --min_word_length, -m: minimum word length, default 3
  --offsite, -o: let the spider visit other sites
  --write, -w file: write the output to the file
  --ua, -u user-agent: useragent to send
  --no-words, -n: don't output the wordlist
  --meta, -a include meta data
  --meta_file file: output file for meta data
  --email, -e include email addresses
```

- Included in Kali
- Creates wordlist from URL, reading words from pages

Crunch

- Generates a wordlist from characters you specify (included in Kali)

```
root@kali:/usr/share/wordlists# crunch
crunch version 3.6

Crunch can create a wordlist based on criteria you specify. The output from crunch can be sent to the screen, file, or to another program.

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use crunch.
root@kali:/usr/share/wordlists# crunch 4 5 AB
Crunch will now generate the following amount of data: 272 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 48
AAAA
AAAB
AABA
AABB
```

Hydra

- Online password cracker
- Can use wordlists or patters

```
root@kali:~/brute# hydra -l root -p password attack.samsclass.info http-get /brute0/
Hydra v7.4.2 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-09-06 14:14:38
[DATA] 1 task, 1 server, 1 login try (l:1/p:1), +1 try per task
[DATA] attacking service http-get on port 80
[80][www] host: 199.188.72.153 login: root password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-09-06 14:14:42
root@kali:~/brute#
```

Offline Password Attacks

Getting the Hashes

- Most operating systems and Web services now hash passwords
 - Although some use plaintext, and most use weak hashing techniques
- Windows stores hashes in an encrypted C:\Windows\SAM file, but the key is available in the SYSTEM file

Two Ways to Strengthen Hashes

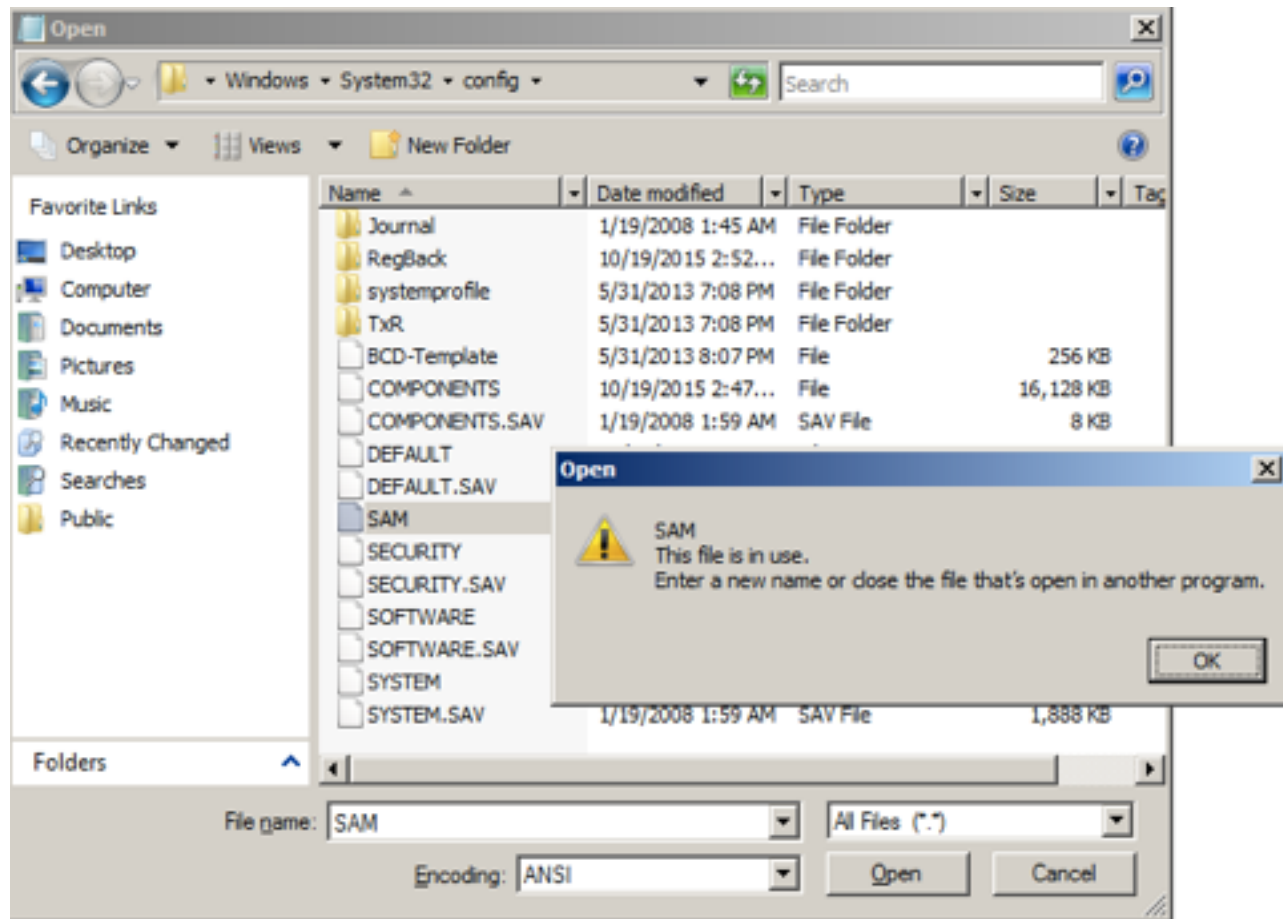
- Salting
 - Add random bytes before hashing
 - Store them with the hash
 - This prevents attackers from pre-computing "Rainbow Tables" of hashes
- Stretching
 - Many rounds, typically 5000, of hashing
 - Slows down attackers

SAM and SYSTEM Files

The screenshot shows a Windows Explorer window titled 'config'. The address bar indicates the path: Local Disk (C:) > Windows > System32 > config. The window displays a list of files and folders with columns for Name, Date modified, Type, and Size. The 'Favorite Links' pane on the left shows standard Windows Explorer shortcuts. The main pane lists several folders and files, including 'Journal', 'RegBack', 'systemprofile', 'TxR', and various system files like 'BCD-Template', 'COMPONENTS', 'COMPONENTS.SAV', 'DEFAULT', 'DEFAULT.SAV', 'SAM', 'SECURITY', 'SECURITY.SAV', 'SOFTWARE', 'SOFTWARE.SAV', 'SYSTEM', and 'SYSTEM.SAV'.

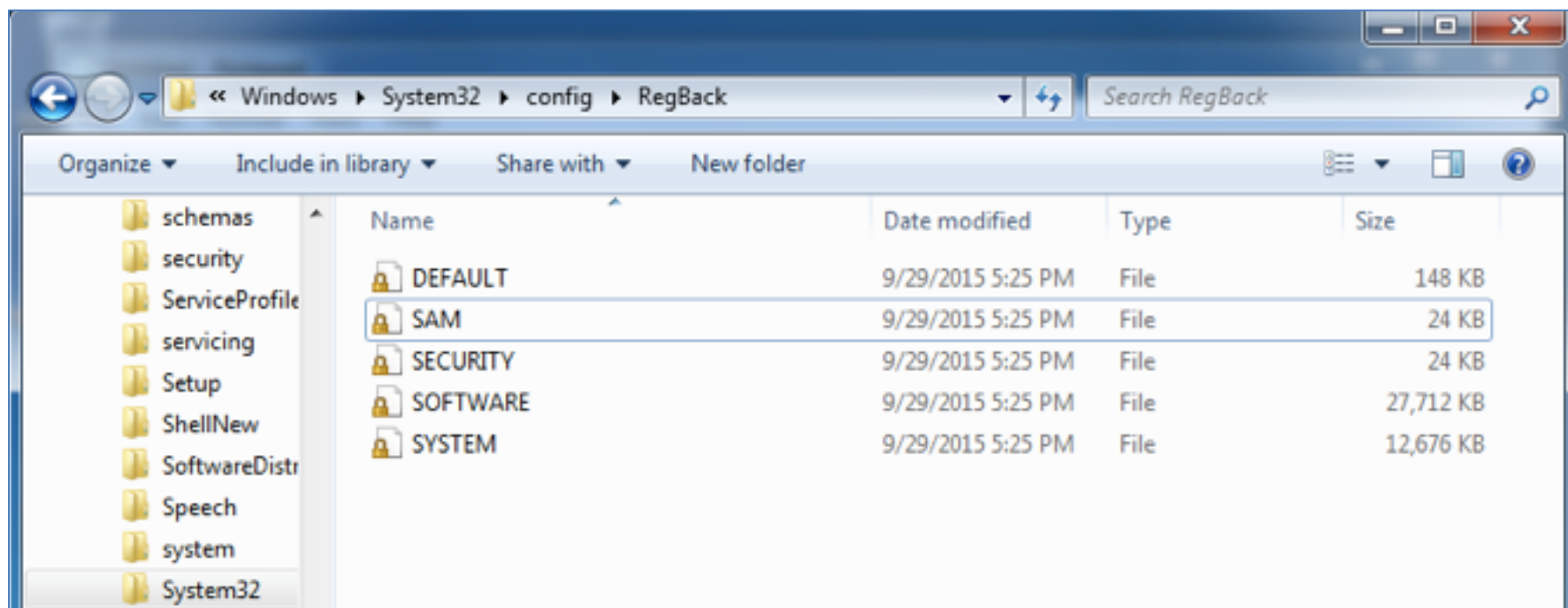
Name	Date modified	Type	Size
Journal	1/19/2008 1:45 AM	File Folder	
RegBack	10/19/2015 2:52 PM	File Folder	
systemprofile	5/31/2013 7:08 PM	File Folder	
TxR	5/31/2013 7:08 PM	File Folder	
BCD-Template	5/31/2013 8:07 PM	File	256 KB
COMPONENTS	10/19/2015 2:47 PM	File	16,128 KB
COMPONENTS.SAV	1/19/2008 1:59 AM	SAV File	8 KB
DEFAULT	10/21/2015 11:03 AM	File	256 KB
DEFAULT.SAV	1/19/2008 1:59 AM	SAV File	20 KB
SAM	10/19/2015 2:46 PM	File	256 KB
SECURITY	10/19/2015 2:47 PM	File	256 KB
SECURITY.SAV	1/19/2008 1:59 AM	SAV File	8 KB
SOFTWARE	10/21/2015 11:03 AM	File	13,568 KB
SOFTWARE.SAV	1/19/2008 1:59 AM	SAV File	9,980 KB
SYSTEM	10/21/2015 11:03 AM	File	12,800 KB
SYSTEM.SAV	1/19/2008 1:59 AM	SAV File	1,888 KB

Unavailable when Windows is Running



Win 7 Backup Files

- Also unavailable when system is running
- Win XP had C:\Windows\Repair but it seems to be gone now



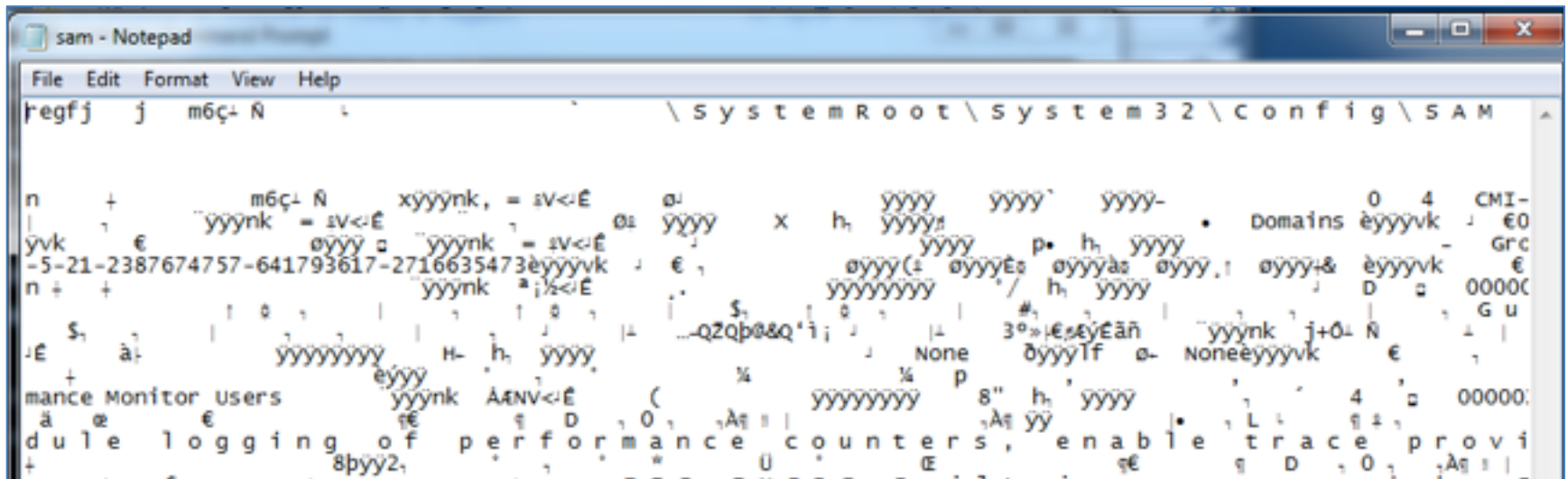
Reg.exe

- Works on Windows 7
 - Link Ch 8i

```
C:\>reg.exe save HKLM\SAM sam
The operation completed successfully
C:\>reg.exe save HKLM\SYSTEM sys
The operation completed successfully
```

SAM is Encrypted

- 128-bit RC4



The image shows a Notepad window titled "sam - Notepad" with the file path "\systemroot\system32\config\sam". The text inside the window is heavily encrypted and appears as a mix of random characters and symbols, including "m6ç± N", "xyyyнк, = sv<E", "Domains", "performance Monitor Users", and "enable logging of performance counters". This visualizes the fact that the SAM file's contents are not readable without the proper decryption key.

Key is in SYSTEM

- apt-get install bkhive FAILS on Kali 2
- Must install old versions of bkhive and samdump2 (link Ch 8l)

```
root@kali:~/124/ch9# bkhive system keyfile
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{F10156BE-0E87-4EFB-969E-5DA29D131144}
Default ControlSet: 001
Bootkey: a8624e8beb93d2e7002c9eb240b53bdb
```

Extracting Hashes

```
root@kali:~/124/ch9# samdump2 sam keyfile
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{899121E8-11D8-44B6-ACEB-301713D5ED8C}
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sam:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:e03c1c4537d9eecbc72074d734b99a19:::
root@kali:~/124/ch9#
```

- LM Hash on the left (now obsolete)
- NT hash on the right (designed in 1991)

Linux Boot Disk

- You can gather hashes by booting the target system from a LiveCD or USB
- Copy the files while Windows is not running

Cracking Windows Passwords

- Hashcat tests 500,000 passwords in a few seconds
 - Because algorithm is 1 round of MD4
 - Proj X16 in CNIT 123

```
root@kali:~/hash# hashcat -m 1000 -a 0 -o winpass1.txt --remove win1.hash rock.dic
Initializing hashcat v0.44 by atom with 8 threads and 32mb segment-size...
Added hashes from file win1.hash: 1 (1 salts)
Activating quick-digest mode for single-hash
NOTE: press enter for status-screen
All hashes have been recovered
```

Kali's Password Hashes

- 5000 rounds of SHA-512 with a salt
- Mac OS X is the same

```
GNU nano 2.2.6 File: /etc/login.defs
ENCRYPT_METHOD SHA512
#
# Only used if ENCRYPT_METHOD is set to SHA256 or SHA512.
#
# Define the number of SHA rounds.
# With a lot of rounds, it is more difficult to brute forcing the password.
# But note also that it more CPU resources will be needed to authenticate
# users.
#
# If not specified, the libc will choose the default number of rounds (5000).
# The values must be inside the 1000-999999999 range.
# If only one of the MIN or MAX values is set, then this value will be used.
# If MIN > MAX, the highest value will be used.
#
# SHA_CRYPT_MIN_ROUNDS 5000
# SHA_CRYPT_MAX_ROUNDS 5000
```

Cracking Kali Hashes

- Can only try 500 words in a few seconds

```
root@kali:~/124/ch9# cat /etc/shadow
root:$6$5bWgpZ9y$oDwaYKkWoXJoi0wClA7BoKwPW3DRaiUSZ4NI5McoZGLR0wNeK.
IL0AxfgYZ61ME50FQyXjP/wcFvH6vZJ5jGA0:16657:0:99999:7:::
```

```
root@kali:~/hash# hashcat -m 1800 -a 0 -o found1.txt --remove crack1.hash 500_pass
words.txt
Initializing hashcat v0.44 by atom with 8 threads and 32mb segment-size...

Added hashes from file crack1.hash: 1 (1 salts)
Activating quick-digest mode for single-hash with salt

NOTE: press enter for status-screen

All hashes have been recovered
```

John the Ripper & Hashcat

- Cracks many types of hashes
 - Auto-detects the algorithm
 - Can perform brute force, or dictionary, or modified dictionary attacks
- Hashcat is newer and claims to be faster
- oclHashcat
 - Designed to run in parallel on many GPUs

CloudCracker

- Moxie Marlinspike's service
- Runs on AWS machines



The screenshot shows the CloudCracker website interface. At the top, the URL is <https://www.cloudcracker.com>. The logo features a blue cloud with a keyhole icon and the text "CloudCracker". Below the logo, a description reads: "An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption."

The main section is titled "Start Cracking" and contains a form with the following fields:

- File Type:** A dropdown menu currently set to "WPA/WPA2".
- Handshake File:** A file selection button labeled "Choose File" with the text "No file chosen" next to it.
- SSID (Network Name):** A text input field with a lock icon on the right, indicating it is a required field.

A green "Next >" button is positioned below the SSID field. At the bottom of the form, there are three tabs: "Handshake", "Dictionary", and "Delivery".

Cheap!



Big. Fast. Cheap.
Run your network
handshake against
300,000,000 words
in 20 minutes
for \$17.

Mimikatz Gets Clear Passwords from RAM

```
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter > kerberos
[!] Not currently running as SYSTEM
[*] Attempting to getprivs
[+] Got SeDebugPrivilege
[*] Retrieving kerberos credentials
kerberos credentials
=====
```

AuthID	Package	Domain	User	Password
-----	-----	-----	----	-----
0;999	NTLM	WORKGROUP	WIN-JWBPPZSXEfv\$	
0;996	Negotiate	WORKGROUP	WIN-JWBPPZSXEfv\$	
0;69395	NTLM			
0;997	Negotiate	NT AUTHORITY	LOCAL SERVICE	
0;150806	NTLM	WIN-JWBPPZSXEfv	Administrator	P@ssw0rd

```
meterpreter > █
```


Stolen Password Lists

Why passwords have never been weaker— and crackers have never been stronger

Thanks to real-world data, the keys to your digital kingdom are under assault.

by Dan Goodin - Aug 20, 2012 6:00pm PDT

 Share

 Tweet

335

- Lists of millions of real stolen passwords are now available
- The rockyou list is included in Kali
 - in /usr/share/wordlists
 - Link Ch 9e

Passphrases are Vulnerable

“thereisnofatebutwhatwemake”—Turbo-charged cracking comes to long passwords

Cracking really long passwords just got a whole lot faster and easier.

by Dan Goodin - Aug 26, 2013 1:44pm PDT

 Share

 Tweet

 280

Cracking 16 Character Strong passwords in less than an hour

Thursday, May 30, 2013 Mohit Kumar

```
4b31e7e74759ad86dd902cf1cba48e7f: isthatbacon
14140c179791b6a44aef4978efc54794: 1234menarmy
7c4c7513058d973f2ad349d9d061b97d: howdoyouthink!
356a2d66f59c30c92dafbc7f68987293: kristyjimmy
9f306ff2a675fcab9b3c9f550a0937a7: 101294master
ce0f292da5f954885c0d28233acec0e4: InsertPassword
1cc7f0c92a9c809b82f8ee1e416d99a7: wadedf789
c43f8bbc95b9e5117f39c666cdc30dc7: simon13jack
472534b9e37674ede3516c0a0bc720d7: samfordpassword
s02b3fc0365807a65ae14cb3e8da818ac: andrew12love
984e5183a5cd1a8958594a7425e05204: recuerdami amor
e2070b253ba489f585717e5abb57d07b: jjeekk44221
e8a7777bc9fb0223d97bb33a83fcdcff: tatorbeta
f24762a3b7a5683c56d459c5cdc84a02: vamosfuerte
```

- Hashed with MD5 (link Ch 9g)

How the Bible and YouTube are fueling the next frontier of password cracking

Crackers tap new sources to uncover "givemelibertyorgivemedeth" and other phrases.

by Dan Goodin - Oct 8, 2013 6:00am PDT

 Share

 Tweet

266

Almost immediately, a flood of once-stubborn passwords revealed themselves. They included: "Am i ever gonna see your face again?" (36 characters), "in the beginning was the word" (29 characters), "from genesis to revelations" (26), "I cant remember anything" (24), "thereisnofatebutwhatwemake" (26), "givemelibertyorgivemedeth" (26), and "eastofthesunwestofthemoon" (25).

- Link Ch 9h

Dumping Passwords from RAM

Plaintext Passwords

- Windows stores the password of the currently logged-on user in RAM with "reversible encryption"
- It can be recovered with Windows Credential Editor or mimikatz
- No matter how long or complex it is

Analysis of Stolen Data Dumped by TEAMGHOSTSHELL on Aug 25, 2012

17. Ok, that's all. Whoever wants any of them, you can contact me at voxanon. (make sure my nick is registered, there are many impostors out there). Oh, and people have kept asking me about the WallStreet hack from MidasBank. We have uploaded it once more here for you and it's also at our friends from Par-AnoIA. (<http://par-anoia.net/midasbank/>) C ya all in the fall - DeadMellox

18.
19. _____
20.

21. CIA Services Part1 - Mirror1 <http://paste.scratchbook.ch/view/raw/c278c8c6> Mirror2 <http://pastehtml.com/view/c9duegpin.txt> Mirror3 <https://pastee.org/54ceq/preview> Mirror4 <http://safebin.net/8217> Mirror5 <https://gist.github.com/f76133bf1c1537cc256a> Mirror6 <http://pastesite.com/42279>

22.
23. CIA Services Part2 - Mirror1 <http://paste.scratchbook.ch/view/0c722b86> Mirror2 <http://pastehtml.com/view/c9dwehy1k.txt> Mirror3 <https://pastee.org/rrxsp> Mirror4 <http://safebin.net/8218> Mirror5 <https://gist.github.com/5f4b53cc3f32c8fa28a0> Mirror6 <http://pastesite.com/42278>

24.
25. CIA Services Part3 - Mirror1 <http://paste.scratchbook.ch/view/f0951561> Mirror2 <http://pastehtml.com/view/c9dwssda3.txt> Mirror3 <https://pastee.org/bsxej> Mirror4 <http://safebin.net/8219> Mirror5 <https://gist.github.com/27154e7f615ee429a172> Mirror6 <http://pastesite.com/42280>

26.
27. CIA Services Part4 - Mirror1 <http://ideone.com/8ezsL> Mirror2 <http://pastehtml.com/view/c9dxb0g3v.txt> Mirror3 <https://pastee.org/mafwa> Mirror4 <http://safebin.net/8220> Mirror5 <https://gist.github.com/482b058434e26800bb67> Mirror6 <http://pastesite.com/42281>

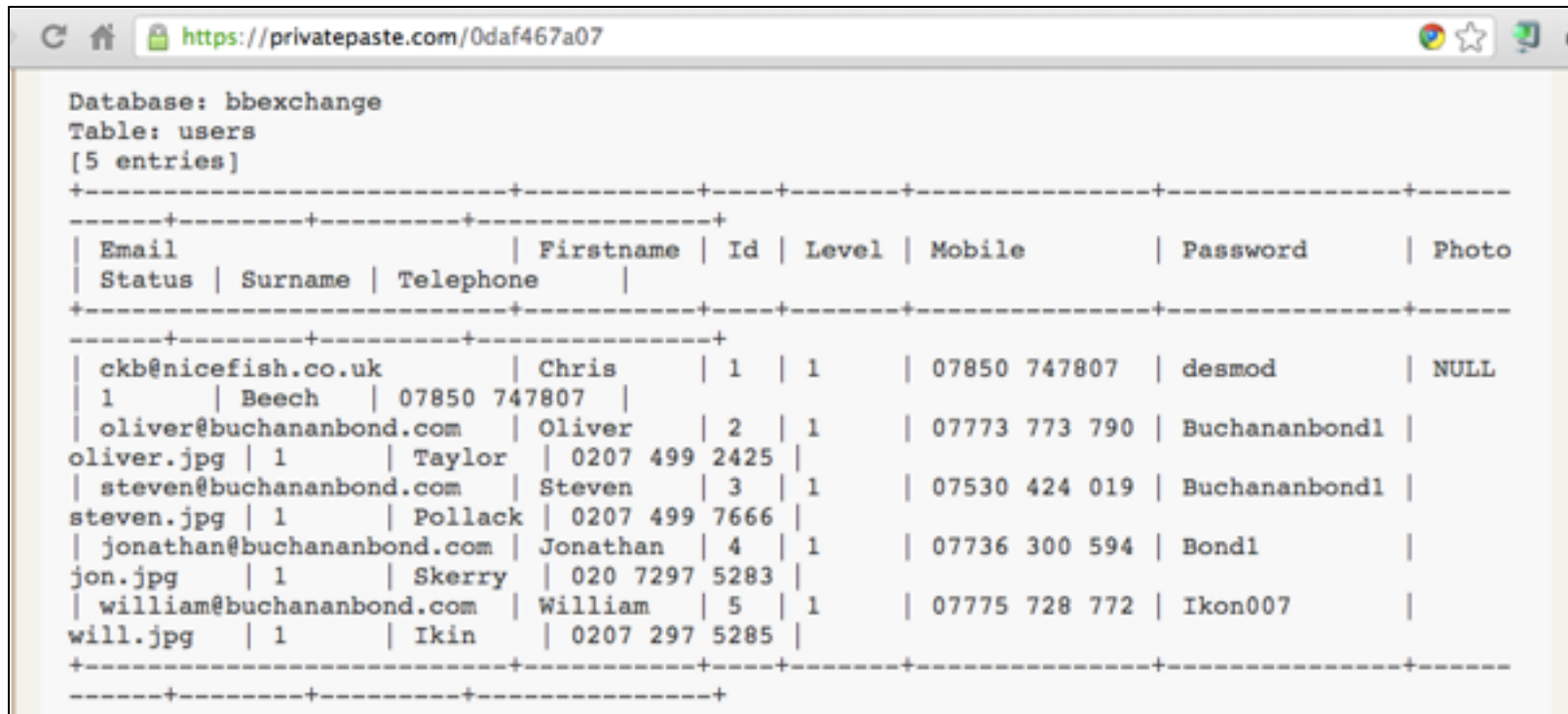
28.
29. CIA Services Part5 - Mirror1 <http://ideone.com/rswyv> Mirror2 <http://pastehtml.com/view/c9dy1fzp8.txt> Mirror3 <https://pastee.org/wptfx> Mirror4 <http://safebin.net/8221> Mirror5 <https://gist.github.com/8b0003c5ac0c03791f98> Mirror6 <http://pastesite.com/42282>

30.
31.
32. GarretGroup Part1 - Mirror1 <https://gist.github.com/01ae21acd58ff65241bf> Mirror2 <http://pastesite.com/42283> Mirror3 <https://privatepaste.com/a36573b3fa>

Password Storage: Awful Beyond Belief

Plaintext, obvious, all the same

Plaintext Passwords, Easily Guessed



The screenshot shows a web browser window with the address bar containing <https://privatepaste.com/0daf467a07>. The main content area displays a database dump for a database named 'bbexchange' and a table named 'users'. The dump indicates there are 5 entries in the table. The data is presented in a table format with columns for Email, Status, Surname, Telephone, Firstname, Id, Level, Mobile, Password, and Photo. The passwords are plaintext and easily guessable.

Email	Status	Surname	Telephone	Firstname	Id	Level	Mobile	Password	Photo
ckb@nicefish.co.uk	1	Beech	07850 747807	Chris	1	1	07850 747807	desmod	NULL
oliver@buchananbond.com	1	Taylor	0207 499 2425	Oliver	2	1	07773 773 790	Buchananbond1	oliver.jpg
steven@buchananbond.com	1	Pollack	0207 499 7666	Steven	3	1	07530 424 019	Buchananbond1	steven.jpg
jonathan@buchananbond.com	1	Skerry	020 7297 5283	Jonathan	4	1	07736 300 594	Bond1	jon.jpg
william@buchananbond.com	1	Ikin	0207 297 5285	William	5	1	07775 728 772	Ikon007	will.jpg

www.rreeves.com

Los Angeles Immigration Attorney - Your Immigration Solutions

Home | Search | Login



OVERVIEW FOUNDER VISAS VISA INFO CLIENTS NEWS ATTORNEYS OFFICES CONTACT

Quick Links

Schedule a Consultation

IMPORTANT UPDATES USCIS WILL SOON BE ACCEPTING APPLICATIONS FOR DEFERRED ...

pastesite.com/42306

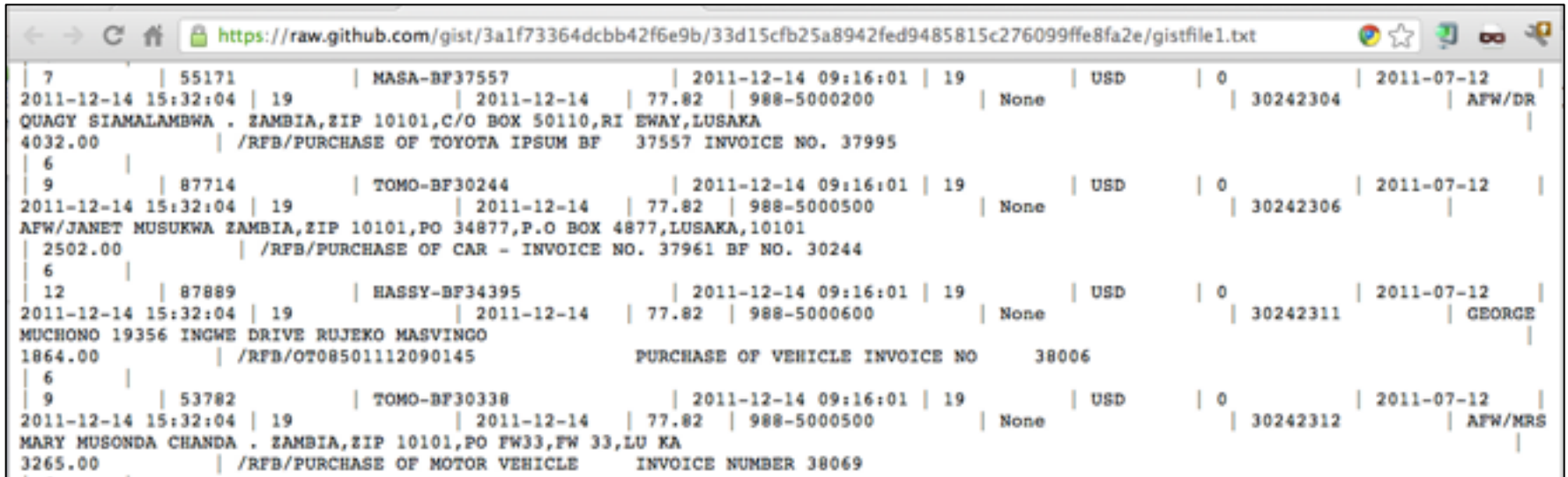
password	pay	position	username
ljlaw321	0	2	Lorraine
dllaw321	0	2	David
1234	0	2	Christy
jllaw321	0	1	jeremiah
1234	0	2	Lilian
1234	0	2	Yan
1234	0	1	Nathan
oslaw321	0	2	Odontuya
oalaw321	0	3	cassie
aclaw321	0	2	Arthur
mllaw321	0	3	manila
123456	0	NULL	steven
1234	0	2	Erlic
fdlaw321	0	1	flomy
Robert	0	1	Robert
iglaw321	0	2	Ivone
bhparalaw	0	2	Bonnie
1234	0	1	Armineh
khlaw321	0	NULL	kathleen
aplaw321	0	1	Anoop
jslaw321	0	1	julie
jslaw321	0	2	Jane
legolas	0	3	shadouh

Sparklan Passwords

Database: sparklan_db
Table: user
[15 entries]

created	flag	modified	user_id	user_mail	user_name	user_password	user_real_name
0000-00-00 00:00:00 1234567 0	0	2006-01-23 23:18:58	1	admin@admin.com	admin	adminpw	administrator
2008-06-23 10:11:10 4343 1	0	2008-06-23 10:11:10	3	isaac.chang@sparklan.com	chelsea	sparklan	isaac
2006-03-08 14:03:14 1212121 1	0	2008-04-30 17:59:53	6	salesinfo@sparklan.com	crisrina	salesinfo	salesinfo
2008-05-19 10:30:06 4343 1	0	2008-05-19 10:30:06	16	salesinfo@sparklan.com	forest	sparklan	salesinfo
2008-06-10 14:13:43 4343 1	0	2008-06-10 14:13:43	17	yiching.shih@sparklan.com	grand	sparklan	yiching
2006-04-11 17:17:19 311 1	0	2006-04-11 17:17:19	25	chelsea.hsu@sparklan.com	isaac	sparklan	chelsea
2008-06-26 14:22:31 43 1	0	2008-06-26 14:22:31	30	ray.chen@sparklan.com	jane	sparklan	ray
2006-07-05 18:03:05 1	0	2006-07-05 18:03:05	31	grand.wu@sparklan.com	marketing	sparklan	grand
2007-02-26 16:49:58 1	0	2007-02-26 16:49:58	32	support@sparklan.com	ray	sparklan	support
2008-06-23 10:10:27 4343 1	0	2008-06-23 10:10:27	33	forest.liu@sparklan.com	register	sparklan	forest
2006-07-05 11:43:00 1	0	2006-07-05 11:43:00	34	register@sparklan.com	sales	sparklan	register
2008-06-23 10:12:51 3434 1	0	2008-06-23 10:12:51	35	sam.tai@sparklan.com	salesinfo	sparklan	sam
2008-06-17 16:30:53 3434 1	0	2008-06-17 16:30:53	36	jane.jian@sparklan.com	sam	sparklan	jane
2008-06-17 17:21:29 4343 1	0	2008-06-17 17:21:29	37	crisrina.teng@sparklan.com	support	sparklan	crisrina
2008-09-02 10:30:24 1 1	0	2008-09-03 09:29:49	38	marketing@sparklan.com	yiching	sparklan	marketing

Beforeward Transactions with PII



The image shows a screenshot of a web browser displaying a list of transactions. The browser's address bar shows the URL: <https://raw.githubusercontent.com/gist/3a1f73364dcb42f6e9b/33d15cfb25a8942fed9485815c276099ffe8fa2e/gistfile1.txt>. The page content is a text-based list of transactions, each with a unique ID, date, time, and various details including names, addresses, and amounts.

ID	Date	Time	Name	Address	Amount	Invoice No.	Vehicle	Year
7	2011-12-14	15:32:04	MASA-BF37557	QUAGY SIAMALAMBWA . ZAMBIA, ZIP 10101, C/O BOX 50110, RI EWAY, LUSAKA	4032.00	37557	TOYOTA IPSUM BF	19
6	2011-12-14	15:32:04	TOMO-BF30244	AFW/JANET MUSUKWA ZAMBIA, ZIP 10101, PO 34877, P.O BOX 4877, LUSAKA, 10101	2502.00	37961	CAR	19
12	2011-12-14	15:32:04	HASSY-BF34395	MUCHONO 19356 INGWE DRIVE RUJEKO MASVINGO	1864.00	38006	VEHICLE	19
9	2011-12-14	15:32:04	TOMO-BF30338	MARY MUSONDA CHANDA . ZAMBIA, ZIP 10101, PO FW33, FW 33, LU KA	3265.00	38069	MOTOR VEHICLE	19

Plaintext Passwords

```
Database: chartco_dalkia
Table: users
[290 entries]
+-----+
+-----+
+-----+
| email | | fullname |
level | mobile | password | position
| skype | | username |
+-----+
+-----+
+-----+
| sviallet@dalkia.ae | | Sebastien VIALLET
| +971 506258199 | | beuz82 | HSEQ manager
| NULL | | sviallet |
| mdarwish@dalkia.ae | | Mohammed Darwish
| NULL | | mohd | NULL
| NULL | | mdarwish |
| rami@dowgroup.com | | Rami Saad Miari
| 76 - 776417 | | ramimiari | Web Developer
| rami.miaril | | ramittoll |
| aabuyousuf@dalkia.ae | | Abdulfattah Abu Yousuf
| NULL | | aabuyousuf | Asset Management
| NULL | | aabuyousuf |
| nsequeira@dalkia.ae | | Naveen Sequeira
| +971-0566178133 | | 265568ab | Asset Management
| NULL | | nsequeira |
```

Password Storage: BASE64

Obfuscated, not hashed

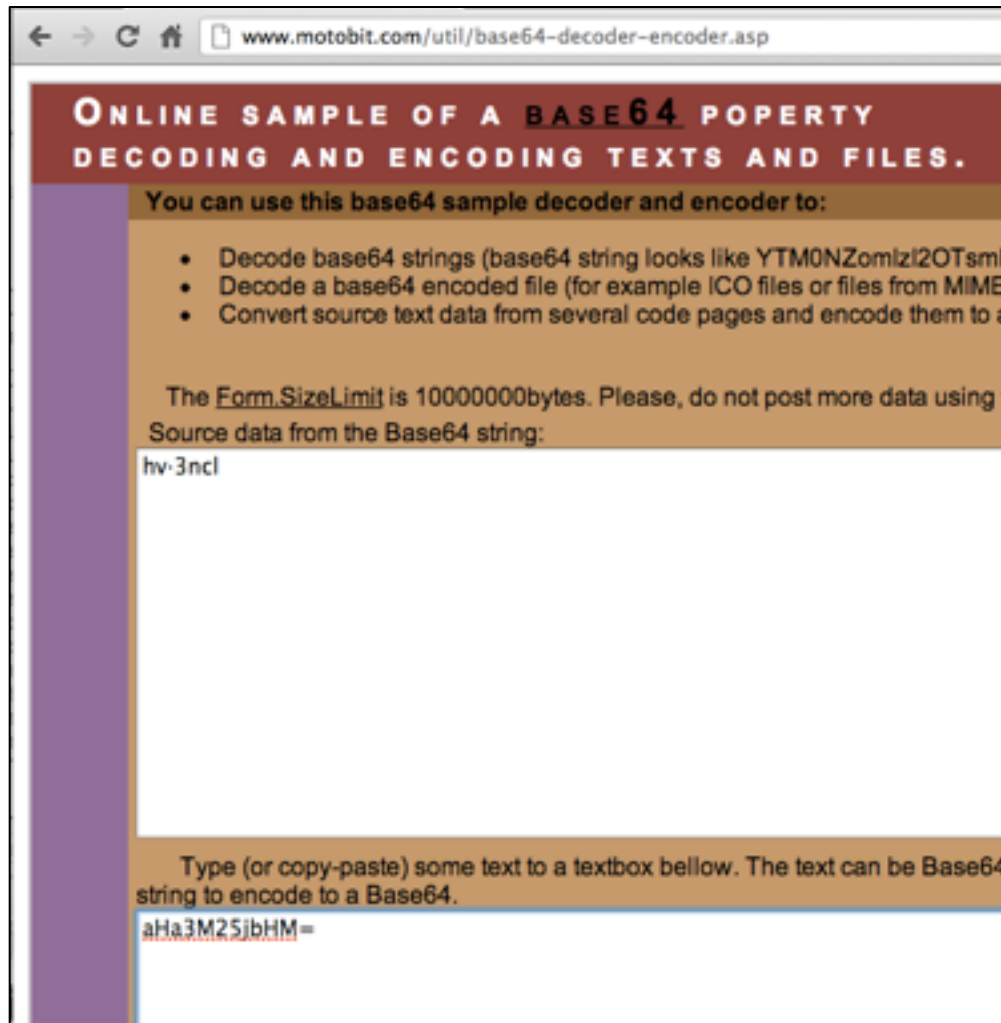
Beforward.jp

Database: i3_beforward
Table: users
[53 entries]

account_no	del_flg	email	first_name	last_name	password		
sort_no2	sort_no3	sort_no4	sort_no5	sort_no6	user_id	user_name	user_type
988-5000100	0	top@beforward.jp	Yasu	None	MzRjd21mZ20=		
404	404	404	404	0	Yasu	1	
None	0	yamakawa@beforward.jp	Hiro	None	eGlvYzVxeDM=		
999	999	999	999	1	Hiro	1	
None	0	suemori@beforward.jp	Taka	None	cnJlN2Njczk=		
999	999	999	999	2	Taka	1	
988-5000300	0	top@beforward.jp	Manabu	None	YjU3b2Z1enI=		
402	402	402	402	3	Manabu	1	
988-5000000	0	top@beforward.jp	Taco	None	aHA3M25jbHM=		
401	401	401	401	4	Taco	1	
None	0	top@beforward.jp	Mitsu	None	Z2g0a2IwdWk=		
999	999	999	9999	5	MITSU	1	
988-5000200	0	top@beforward.jp	Masa	None	N2J6bmFwNHY=		
403	403	403	403	6	Masa	1	

6.1 We employ commercially reasonable security methods to prevent unauthorized access, maintain data accuracy and ensure correct use of information.

BASE64 Encoding



The screenshot shows a web browser window with the address bar displaying `www.motobit.com/util/base64-decoder-encoder.asp`. The page has a dark red header with the text "ONLINE SAMPLE OF A BASE64 PROPERTY DECODING AND ENCODING TEXTS AND FILES." Below the header, a brown box contains the text "You can use this base64 sample decoder and encoder to:" followed by a bulleted list: "• Decode base64 strings (base64 string looks like YTM0NZomlzi2OTsm)", "• Decode a base64 encoded file (for example ICO files or files from MIME)", and "• Convert source text data from several code pages and encode them to a". Below this, a note states "The `Form.SizeLimit` is 10000000bytes. Please, do not post more data using Source data from the Base64 string:". A large white text area contains the input string `hw-3ncl`. At the bottom, another brown box says "Type (or copy-paste) some text to a textbox bellow. The text can be Base64 string to encode to a Base64.", and a final white text area contains the output string `aHa3M25jbHM=`.

← → ↻ 🏠 📄 www.motobit.com/util/base64-decoder-encoder.asp

ONLINE SAMPLE OF A BASE64 PROPERTY DECODING AND ENCODING TEXTS AND FILES.

You can use this base64 sample decoder and encoder to:

- Decode base64 strings (base64 string looks like YTM0NZomlzi2OTsm)
- Decode a base64 encoded file (for example ICO files or files from MIME)
- Convert source text data from several code pages and encode them to a

The `Form.SizeLimit` is 10000000bytes. Please, do not post more data using Source data from the Base64 string:

hw-3ncl

Type (or copy-paste) some text to a textbox bellow. The text can be Base64 string to encode to a Base64.

aHa3M25jbHM=

Password Storage: Unsalted MD5 or SHA-1

Real hashing, but very easy to
crack

MIT - MD5 Password Hashes

```
safebin.net/8222
```

171.	Database: materials	
172.	Table: tbl_mit_modul_users	
173.	[26 entries]	
174.	-----+-----	
175.	password	username
176.	-----+-----	
177.	15ec04b902a94abb0abdc7c3455a9082	rkemper@mit.edu
178.	8d066a766c3991bee2dcfef1847d7b36	jlandry@mit.edu
179.	ac404c90f9952be32e7ac004ff977cf9	lmayer@MIT.EDU
180.	fff83b933071d358c88149f9a0f4d21d	aglietti@MIT.EDU
181.	9b656fall15ale5b9f41f1f98a5727a92	rsa@MIT.EDU
182.	0c76f3625b9987550b0aae5325a3e904	mtim@MIT.EDU
183.	417e7aad3b19791275bb97399ff853ee	pboisver@MIT.EDU
184.	ce0816e26302c5335f2158fc5f99142c	yzhang05@MIT.EDU
185.	4875dc668efbcb7f92b1b48b2b336481	speakman@MIT.EDU
186.	c30fde34d9759760c4f0b6599fd58692	sc79@MIT.EDU
187.	90a3e0e7af307cf631ec83fc06b63800 (hiawatha)	elshaw@MIT.EDU
188.	f37a811c53a8b7656ac79a39e09efd39	mbeals@MIT.EDU
189.	437cf0b95453e22c351e2e031e0778d1	tatem@MIT.EDU
190.	87260b4fff690434a0f91d63511f98bc	diadiuk@MIT.EDU
191.	7f13daaf54c875ae01193401e76743b0	mondol@nano.mit.edu
192.	5239ccd2aaca371c13118d1705647b48	gpetrich@MIT.EDU
193.	7b03d3bd7c900a377a8a6d0c113bf52b	alan_s@MIT.EDU
194.	8873d423e54e527201d03e3176d47d9b	krystyn@MIT.EDU
195.	37c9279d3fe9a0ae55f50874f1dedf0a	watson@wi.mit.edu
196.	c5ale49a6ead8b95eb84129cc2360663	sdalton@MIT.EDU
197.	90a242d8e9f077e03ae9b9e9c2d1fa10	gedik@MIT.EDU
198.	2cdcde61ccddabdec5342e7d72849819	strano@mit.du
199.	512a85775a359512123675f9c36de535	pjarillo@MIT.EDU
200.	a7fed65ed81dc7bb821a43791afabbae	asphodel@MIT.EDU
201.	al354c3049f22725d7b07ddccf7f146d	t_gray@MIT.EDU
202.	ea80e7b94d9077c0cdf28a001e41996b	mpearrow@MIT.EDU
203.	-----+-----	



MD5Decrypter.co.uk

IRC: irc.freenode.net
Channel: #md5decrypter

Use SSL, (Secure Socket Layer)

Check us out on:

- Visit Forum
- MD5 Decrypter
- NTLM Decrypter
- SHA1 Decrypter
- My Hash Lists**
- Hash a Password
- Facebook Hack
- Text Encryption
- List Tool
- Bin Translator
- Downloads
- Statistics
- Upload Passwords
- Rainbow Tables
- Passwd Dump
- NT PW Recovery
- Sam Inside
- Cain & Able
- Port Scanners
- Security News

» What does this MD5 Decrypter tool do?

MD5Decrypter.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

Need more help finding your hashes?

Submit your hashes into **My Hash Lists** from the menu and get dedicated crackers to help you. You need to be registered with our forums in order to use this feature.

How many decryptions are in your database?
We have a total of just over **8.7 billion** unique decrypted MD5 hashes since August 2007.

Please input the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replaced with [space]:

Status: Hashes were found! Please find them below...

MD5 Hashes:
Max: 16
Please use a standard list format

```
ac404c90f9952be32e7ac004ff977cf9 MD5: vorg7r5a
```

Please note the password is after the : character, and the MD5 hash is before it.

abc123

[Load new captcha](#)

Security at MIT: Report an Incident

Get Help > Security at MIT: Report an Incident

Get Help

This form will send email to members of MIT's [Security Support Team](#). Contact them if your issue falls into one of the following four categories:

General IT Security Issue

- You have questions on general IT security topics
- You suspect to have had a network intrusion or other IT security incident

Sensitive Data Issue

- You suspect there has been a data breach in which legally protected data was accessed without authorization

MySQL323 Password Hashes



Database: datas
Table: tbadmin
[2 entries]

adminName	adminPass	adminRating	id
365tech	16925f446f08d646	1,2,3	2
protvinc	110eef2b2f1ac8c8	1,2,3	3

Cracking Hashes with Cain

The screenshot shows the main interface of Cain & Abel. On the left is a tree view of various hash types, including VNC-3DES, MD2, MD4, MD5, SHA-1, SHA-2, RIPEMD-160, Kerb5 PreAuth, Radius Shared-Key, IKE-PSK, MSSQL, MySQL (1), Oracle, Oracle TNS, SIP, 802.11 Captures, WPA-PSK, WPA-PSK Auth, and CHAP. The main window displays a table of captured hashes with the following columns: Username, Password, Hash, challenge, Type, and Note. A single entry is visible with a red 'X' icon in the Username column, the value 'a', and a Hash of '16925F446F08...'. A 'Brute-Force Attack' dialog box is overlaid on the table, showing configuration options for the attack.

Username	Password	Hash	challenge	Type	Note
X a		16925F446F08...		v3.23	

Brute-Force Attack

Charset: Predefined
[abcdefghijklmnopqrstuvwxyz0123456789] Custom

Password length: Min: 1, Max: 16

Start from: []

Keyspace: 8.1860514273734411E+024

Current password: m26ai

Key Rate: 16624887 Pass/Sec

Time Left: 1.56138e+010 years

http://www.oxid.it

SHA-1 Hash

```
Database: industri_web
Table: members
[1 entry]
+-----+-----+-----+
| email      | name      | password                                     |
+-----+-----+-----+
| industrial | Admin User | e6ae401ee24a014f691bc260fe77b62e03be0e1d |
+-----+-----+-----+
```

Cracked!

The screenshot shows the MD5decrypter.co.uk website interface. The browser address bar displays the URL `www.md5decrypter.co.uk/sha1-decrypt.aspx`. The page header includes the site logo, a search bar with the text `9554918457AAAF9929C228C091EAE302`, and IRC information: `IRC: irc.freenode.net` and `Channel: #md5decrypter`. A navigation menu on the left lists various tools such as `Visit Forum`, `MDS Decrypter`, `NTLM Decrypter`, `SHA1 Decrypter`, `My Hash Lists`, `Hash a Password`, `Facebook Hack`, `Text Encryption`, `List Tool`, `Bin Translator`, `Downloads`, `Statistics`, `Upload Passwords`, `Rainbow Tables`, `Passwd Dump`, `NT PW Recovery`, `Sam Inside`, `Cain & Able`, and `Port Scanners`.

The main content area features a tab titled `What does this SHA1 / MySQL Decrypter tool do?`. Below the tab, there are two columns of text. The left column explains the tool's functionality: `MD5Decrypter.co.uk allows you to input an SHA1 / MySQL hash and search for its decrypted state in our database, basically, it's a SHA1 / MySQL cracker / decryption tool.` It also provides statistics: `How many decryptions are in your database? We have a total of just over 8.7 billion unique decrypted SHA1 hashes since December 2009.` The right column asks `Need more help finding your hashes?` and suggests submitting hashes to `My Hash Lists`.

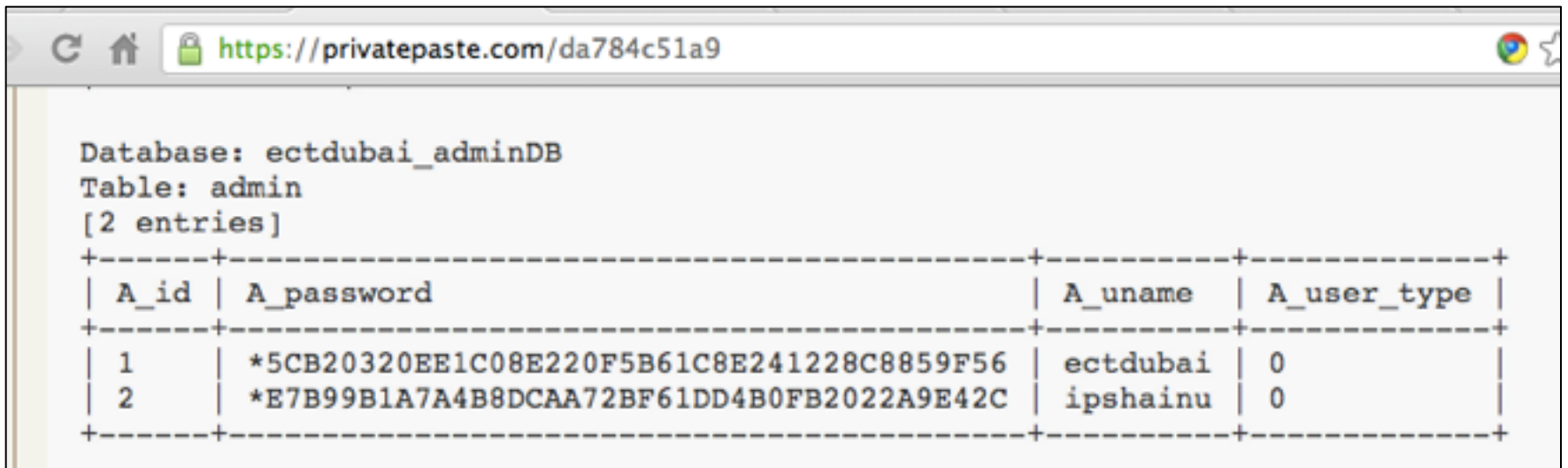
The main input area contains the following text: `Please input the SHA1 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replaced with [space]:`

The `Status:` field displays a green message: `Hashes were found! Please find them below...`

The `SHA1 Hashes:` field contains the input hash: `e6ae401ee24a014f691bc260fe77b62e03be0e1d`. Below this, it specifies `Max: 16` and provides instructions: `Please use a standard list format`.

The output area shows the result: `e6ae401ee24a014f691bc260fe77b62e03be0e1d SHA1: ben24690740`.

MySQL 5 Password Hashes



The screenshot shows a web browser window with the address bar containing <https://privatepaste.com/da784c51a9>. The main content area displays the output of a MySQL query, showing the database name, table name, and two entries from the 'admin' table. The entries are presented in a table format with columns for ID, password hash, username, and user type.

```
Database: ectdubai_adminDB
Table: admin
[2 entries]
```

A_id	A_password	A_uname	A_user_type
1	*5CB20320EE1C08E220F5B61C8E241228C8859F56	ectdubai	0
2	*E7B99B1A7A4B8DCAA72BF61DD4B0FB2022A9E42C	ipshainu	0

Wordpress Password Hashes

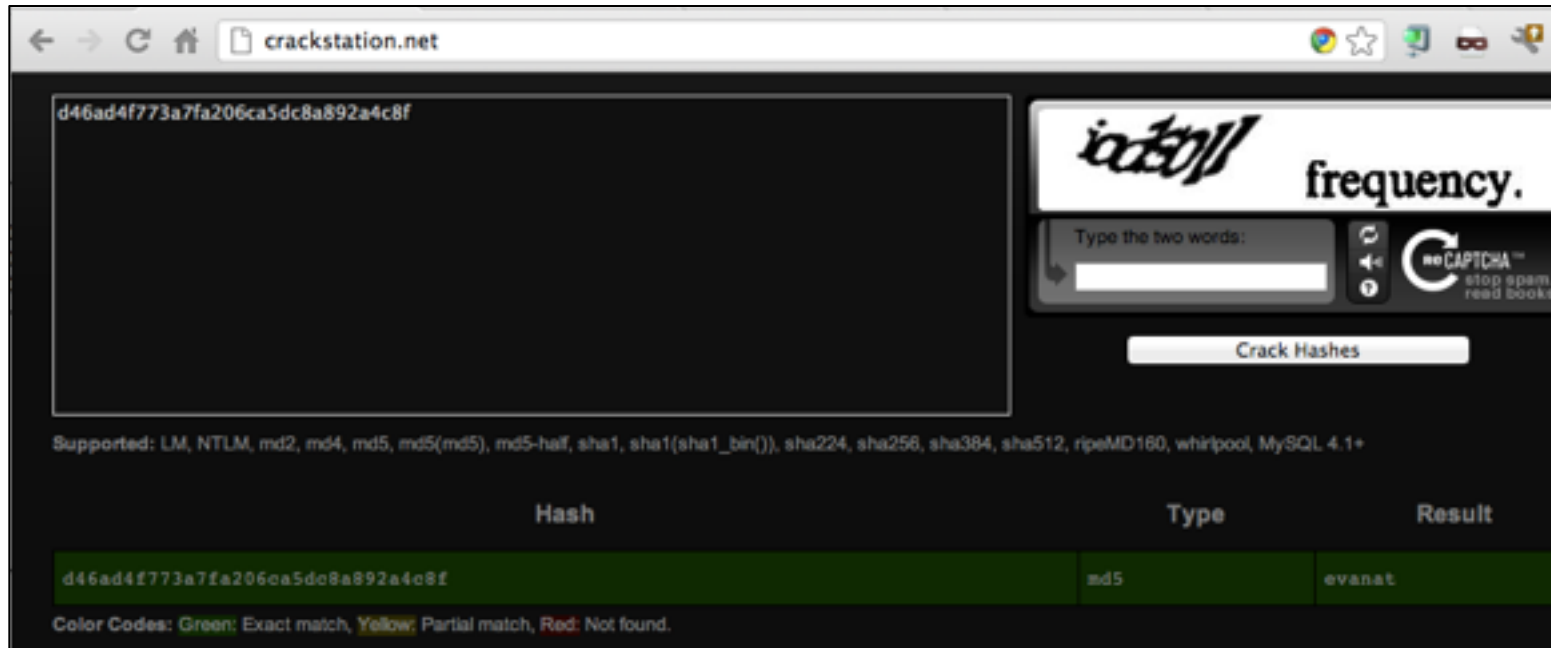
```
90 Database: admin_fairfield
91 Table: wp_users
92 [11 entries]
93 +-----+
94 | user_pass |
95 +-----+
96 | $P$Bv8RJjw3kUa/S2zL00DHWr8wzfwhvn/ |
97 | $P$BX7EY6r8g6jMrqW/dqVNgJYy3XPS0h1 |
98 | $P$B2vHD5YkxNDjJPhwU2BD3IKVQcTqNQ. |
99 | $P$B12uUaVXwlhrNmDqv.9hlNeENpVL1j/ |
100 | $P$BB9jUUzfKEsqATC1NNYafHBpRnb3gO/ |
101 | $P$BBQI0iDaK0DkMlPwVNs/W2AfMSqauQ0 |
102 | $P$BdfpK2bRLbtL2iVdqdrOkEB5Oooxl4. |
103 | $P$BSodk98WYMZ5gRnlw3eRfwsL/AI4pD1 |
104 | $P$ByQWgaJcduJCwetiwn6IPYxpBZwQOf. |
105 | $P$BfRC.WtxdiW0JTcGAF18nUtXx59iPP. |
106 | $P$BH6.WYe22jrhSrDKdSJYJF6isKa/Kl. |
107 +-----+
```

Relative Space



	password
01_02,01_03,	bf00db936e88aalf4c740de064960ecc (chicken2)
01_02,01_03,	b329f324cc17d6221a385ealafb3a289 (marine)
01_03,	bf00db936e88aalf4c740de064960ecc (chicken2)
	d46ad4f773a7fa206ca5dc8a892a4c8f



Cracked!



The screenshot shows a web browser window with the URL `crackstation.net`. The main content area displays a large text box containing the hash `d46ad4f773a7fa206ca5dc8a892a4c8f`. To the right, there is a logo for 'ic3011 frequency.' and a 'noCAPTCHA' widget with the text 'stop spam, read books'. Below the widget is a 'Crack Hashes' button. Underneath the button, a list of supported hash types is shown: 'Supported: LM, NTLM, md2, md4, md5, md5(md5), md5-half, sha1, sha1(sha1_bin()), sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+'. At the bottom, a table displays the results of the cracking process.

Hash	Type	Result
d46ad4f773a7fa206ca5dc8a892a4c8f	md5	evanat

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

→ ↻ 🏠 📄 pastebin.com/BuabHTvr  

```
21. CIA Services Part1 - Mirror1 http://paste.scratchbook.ch/view/raw/c278c8c6 Mirror2
    http://pastehtml.com/view/c9duegpin.txt Mirror3 https://pastee.org/54ceq/preview Mirror4 http://safebin.net/8217
    Mirror5 https://gist.github.com/f76133bf1c1537cc256a Mirror6 http://pastesite.com/42279
22.
23. CIA Services Part2 - Mirror1 http://paste.scratchbook.ch/view/0c722b86 Mirror2
    http://pastehtml.com/view/c9dwehy1k.txt Mirror3 https://pastee.org/rrxsp Mirror4 http://safebin.net/8218 Mirror5
    https://gist.github.com/5f4b53cc3f32c8fa28a0 Mirror6 http://pastesite.com/42278
24.
25. CIA Services Part3 - Mirror1 http://paste.scratchbook.ch/view/f0951561 Mirror2
    http://pastehtml.com/view/c9dwssda3.txt Mirror3 https://pastee.org/bsxej Mirror4 http://safebin.net/8219 Mirror5
    https://gist.github.com/27154e7f615ee429a172 Mirror6 http://pastesite.com/42280
26.
27. CIA Services Part4 - Mirror1 http://ideone.com/8ezsl Mirror2 http://pastehtml.com/view/c9dxb0g3v.txt Mirror3
    https://pastee.org/mafwa Mirror4 http://safebin.net/8220 Mirror5 https://gist.github.com/482b058434e26800bb67
    Mirror6 http://pastesite.com/42281
28.
29. CIA Services Part5 - Mirror1 http://ideone.com/rswyv Mirror2 http://pastehtml.com/view/c9dy1fzp8.txt Mirror3
    https://pastee.org/wptfx Mirror4 http://safebin.net/8221 Mirror5 https://gist.github.com/8b0803c5ac0c03791f98
    Mirror6 http://pastesite.com/42282
```

```

1 Database: 327300_cia
2 Table: contacts
3 [1103 entries]
4 +-----+-----+
5 | first_name          | last_name          |
6 +-----+-----+
7 | Charles             | Sears              |
8 | Richard B & Angela  | Austin             |
9 | Allan               | Darnell            |
10 | Cecilia              | Bodey              |
11 | William and Brenda  | Taylor             |
12 | Matthew              | Greenwood          |
13 |                      | Karasiewicz        |
14 |                      | Sen                 |

```

← → ↻ 🏠 📄 pastehtml.com/view/c9dwehy1k.txt

```

Database: 327300_cia
Table: contacts
[672 entries]
+-----+
| address
+-----+
| 410 Seaborough
| 19827 Dawn Mist Dr
| 6127 Emberwood Falls Dr ,
| 4707 Black Stone
| 4014 n. beechwood court
| 3007 Barnhill Lane
| 13303 White Cliff Dr., Houston, Tx. 77065
| 115 PR 1741
| 1138 E Hampton Dr

```

pastesite.com/42281

teSite.Com

About Recent Pastes Login/Register Contact Terms of Service

Sign Up!
 Pastesite is open to the public, but with limited features. [Register](#) to be able to modify access rights, track your pastes and more...

Change the theme
 If you prefer reading light text on a dark background to dark text on a light background, then you might want to try the [dark theme](#).

Anonymous [Plain Text]

```

1 Database: 327300_cia
2 Table: contacts
3 [655 entries]
4 +-----+-----+-----+
5 | mobile              | phone              | phone2             |
6 +-----+-----+-----+
7 | NULL                | 281-990-0969       | NULL               |
8 | NULL                | 9733772165         | NULL               |
9 | NULL                | 8324237729         | NULL               |
10 | NULL                | 281-862-9585       | NULL               |
11 | NULL                | 6785760932         | NULL               |
12 | NULL                | 281-565-8877       | 832-755-6962      |
13 | NULL                | 979-422-3051       | NULL               |
14 | NULL                | 419-408-7408 cell  | 419-819-6624 cell |
15 | NULL                | 8324664781         | NULL               |
16 | NULL                | 832-276-2104       | NULL               |
17 | NULL                | 281- 207-6052     | NULL               |

```


Password Hashing Algorithms

Hashing Passwords

- Three essential steps
 - One-way hash function
 - MD5, SHA-1, SHA-256, etc.
 - Salt
 - Random characters added to each password
 - Prevents rainbow-table attack
 - Stretching
 - Repeat the hash function many times (typically 5000)
 - Make it take 50 ms to calculate the hash
 - Minimally slows login
 - Makes attack MUCH slower



HACKAHOLIC

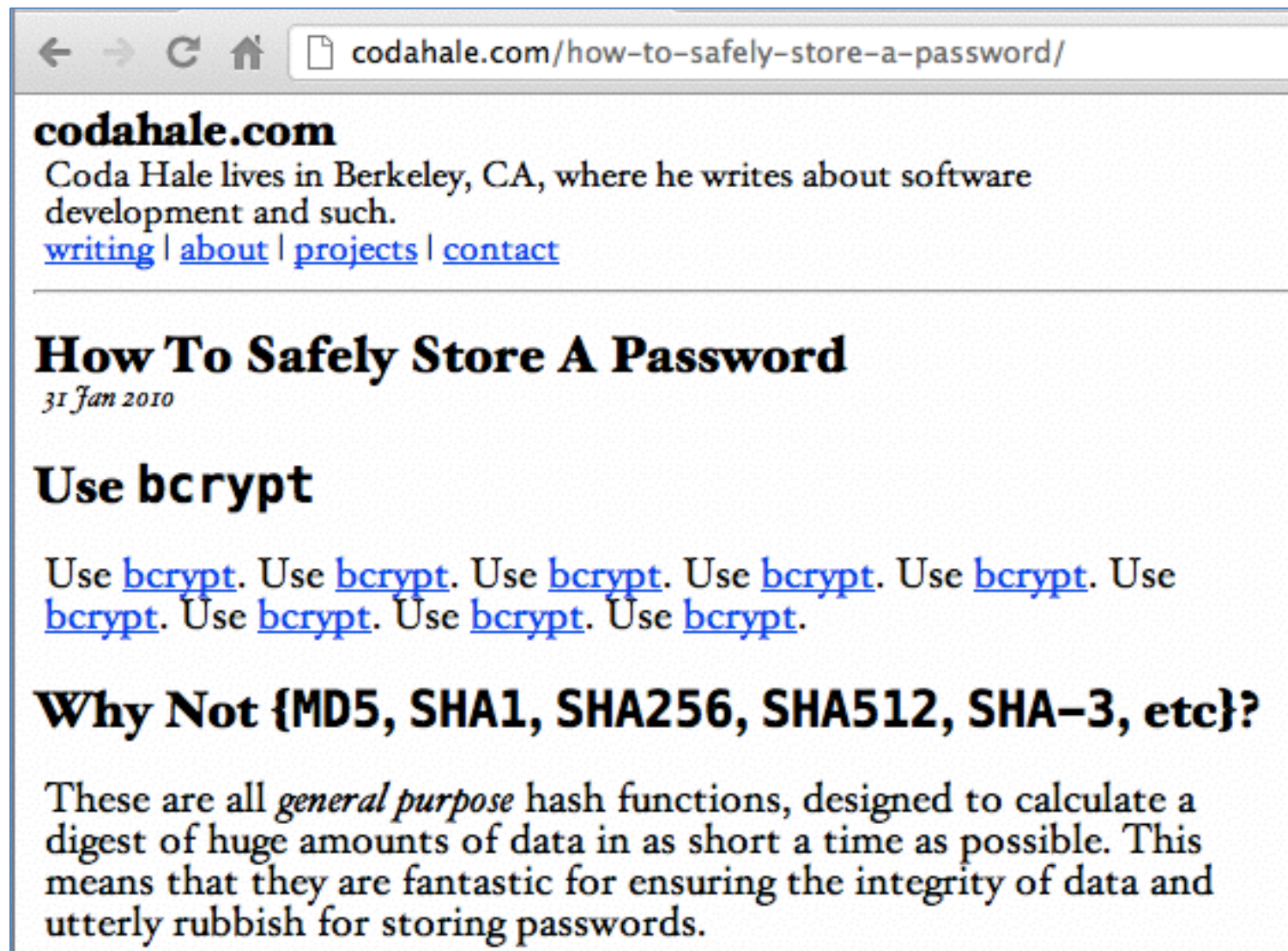
Ethical hacking | Cybersecurity

Browse » [Home](#) » [tutorials](#) » [Different Types of Hashes and Salts](#)

Different Types of Hashes and Salts

Posted by John (Admin) on 2:21 AM | Tags : [Articles](#), [Cryptography](#), [How to](#), [tutorials](#)

The Right Way



The image is a screenshot of a web browser window. The address bar shows the URL "codahale.com/how-to-safely-store-a-password/". The page content includes the site name "codahale.com", a bio for Coda Hale, a list of navigation links, a main article title "How To Safely Store A Password" with a date "31 Jan 2010", a sub-header "Use bcrypt", a paragraph of repeated "Use bcrypt." text, and a section titled "Why Not {MD5, SHA1, SHA256, SHA512, SHA-3, etc}?" followed by a paragraph explaining why these hash functions are not suitable for password storage.

← → ↻ 🏠

codahale.com
Coda Hale lives in Berkeley, CA, where he writes about software development and such.
[writing](#) | [about](#) | [projects](#) | [contact](#)

How To Safely Store A Password

31 Jan 2010

Use bcrypt

Use [bcrypt](#). Use [bcrypt](#). Use [bcrypt](#). Use [bcrypt](#). Use [bcrypt](#). Use [bcrypt](#). Use [bcrypt](#). Use [bcrypt](#). Use [bcrypt](#).

Why Not {MD5, SHA1, SHA256, SHA512, SHA-3, etc}?

These are all *general purpose* hash functions, designed to calculate a digest of huge amounts of data in as short a time as possible. This means that they are fantastic for ensuring the integrity of data and utterly rubbish for storing passwords.

Popular Password Hashes

Type	Projected time to crack 1,000 hashes*	Hash Function	Salt (# chars)	Stretching (# rounds)
Drupal 7	1.7 years	SHA-512	8	16385
Linux (Debian)	58 days	SHA-512	8	5000
Wordpress 3.5.1	17 hours	MD5	8	8193
Windows (all current versions)	5.4 min	MD4	None	1
Joomla	4.6 min	MD5	16	1

- Calculation assumes the passwords are found in a dictionary of 500,000 guesses
- One virtual machine running Kali
- A clusters of GPUs would be much faster