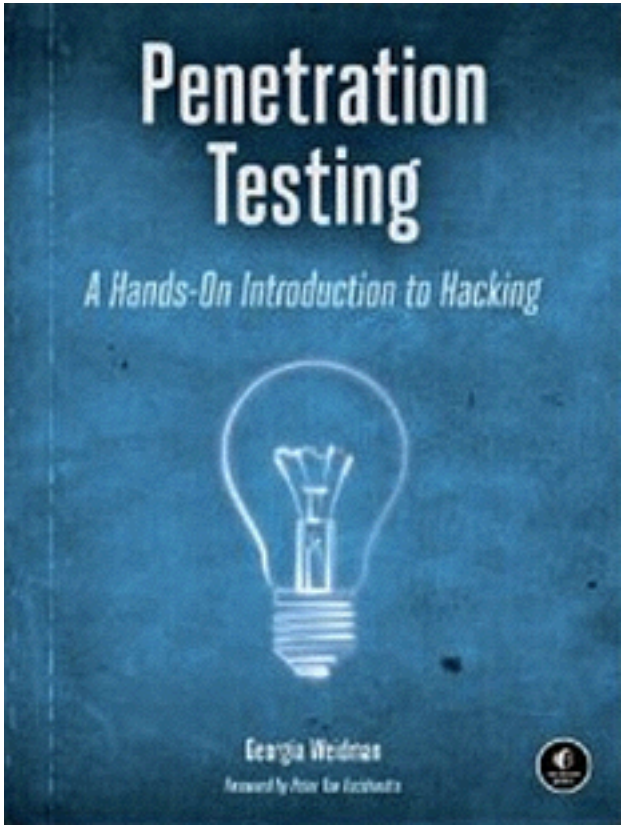
CNIT 124: Advanced Ethical Hacking



Ch 9: Password Attacks

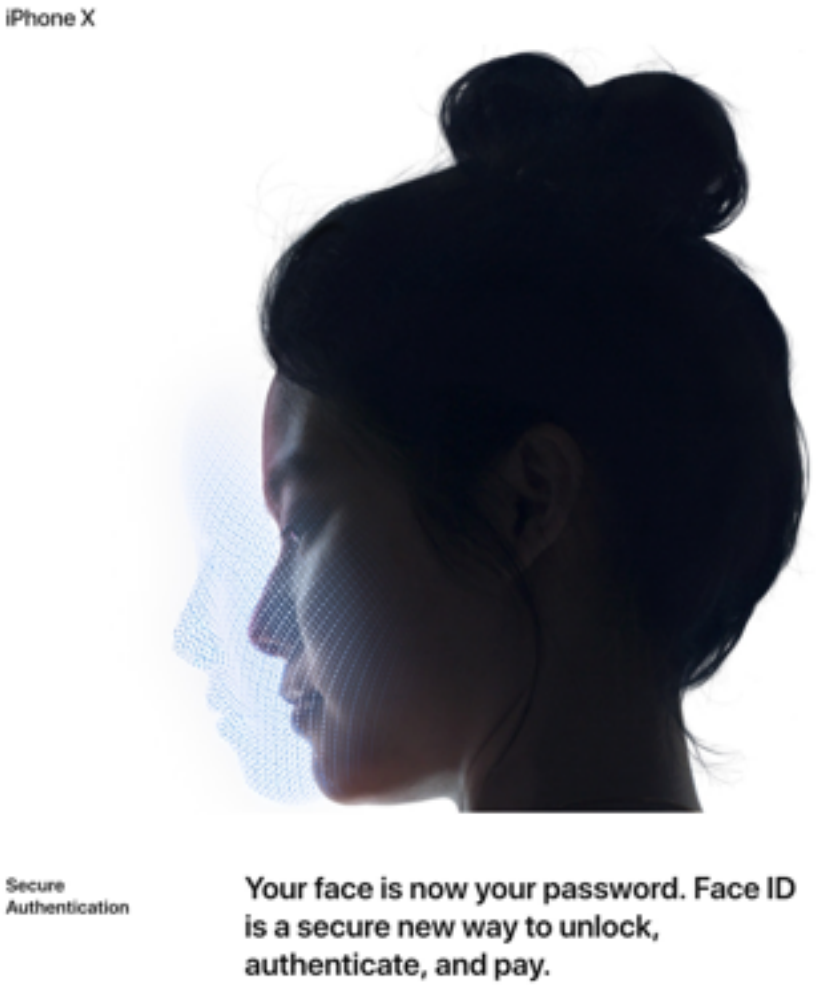
Topics

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

Password Management

Password Alternatives

- Biometrics
- Two-factor authentication
- Digital certificates



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

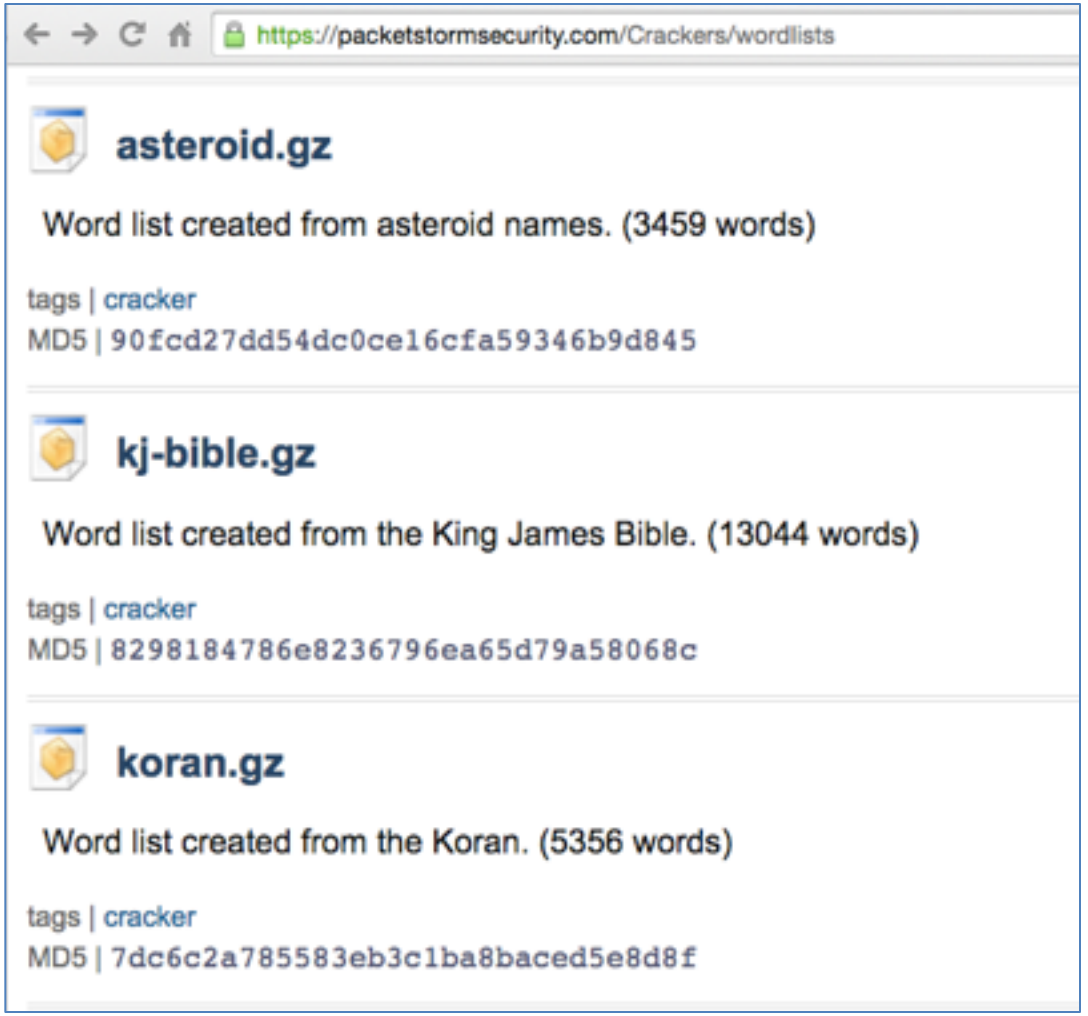
- Scripts try to login with passwords from a list
- Can be blocked by **lockout policies**
  - After five failed logins, must wait an hour
- Brute-forcing is possible
  - Trying every combination of characters
  - Impractical except for very short passwords

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



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

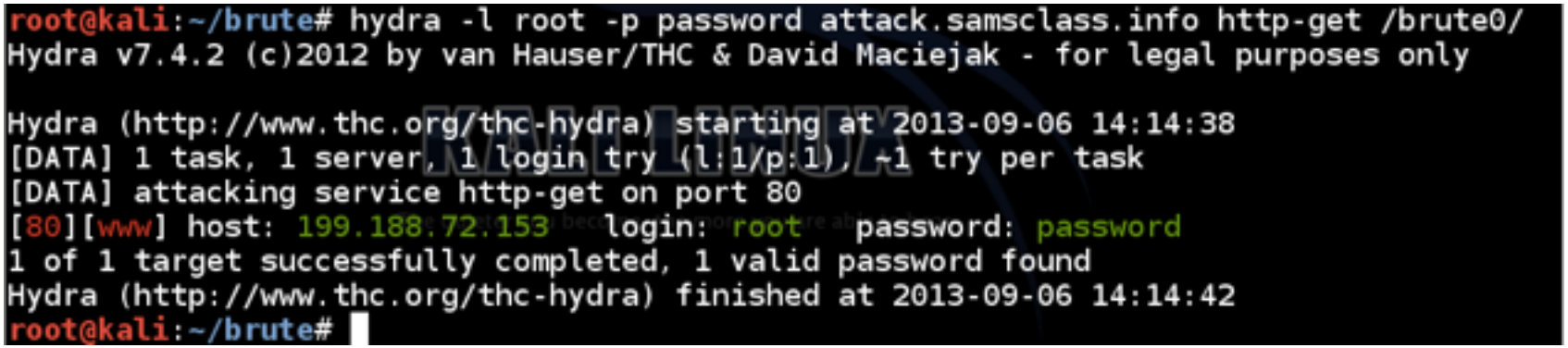
Crunch

- 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 cru
nch 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 pattens



Offline Password Attacks

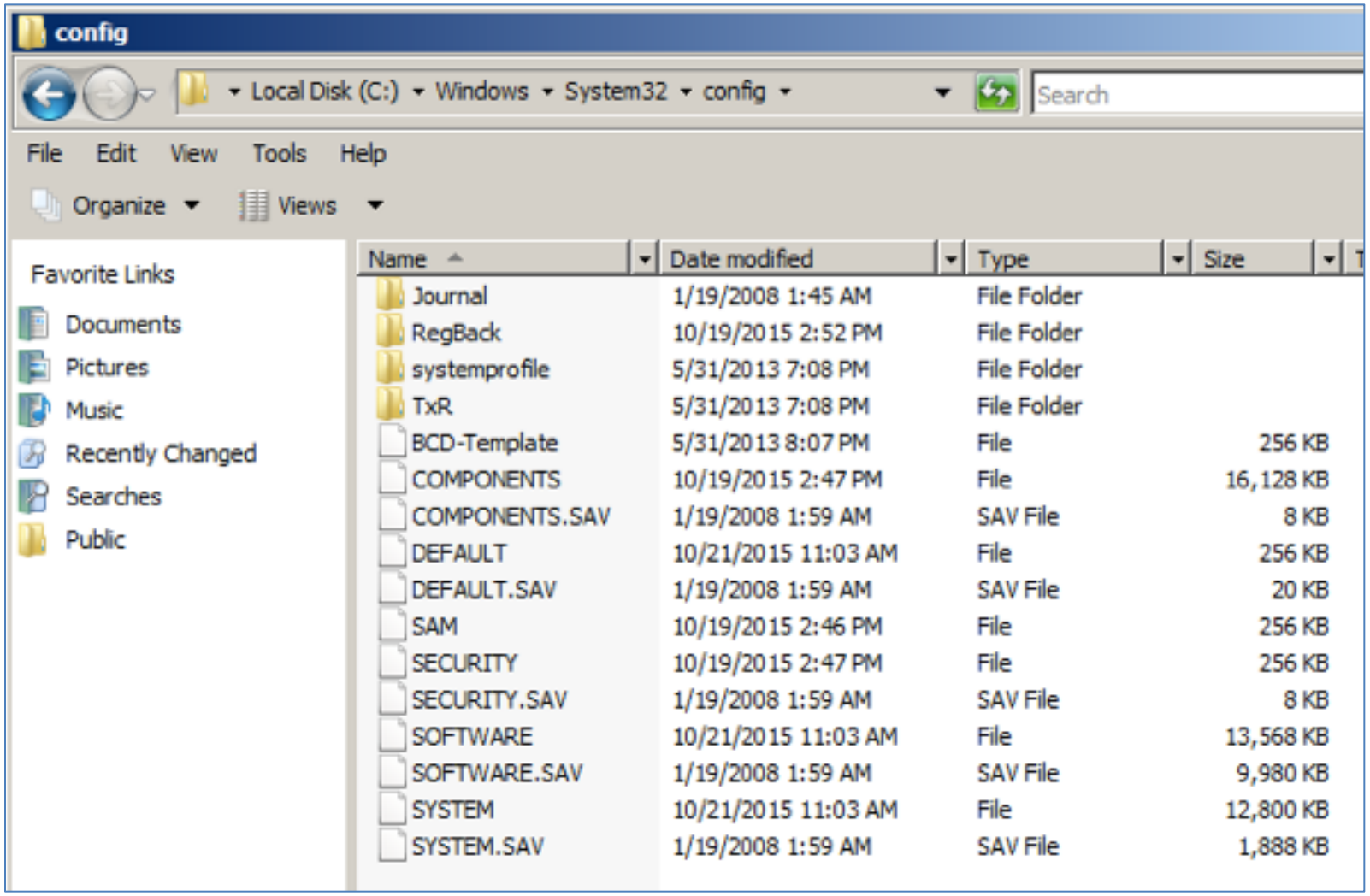
Getting the Hashes

- 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

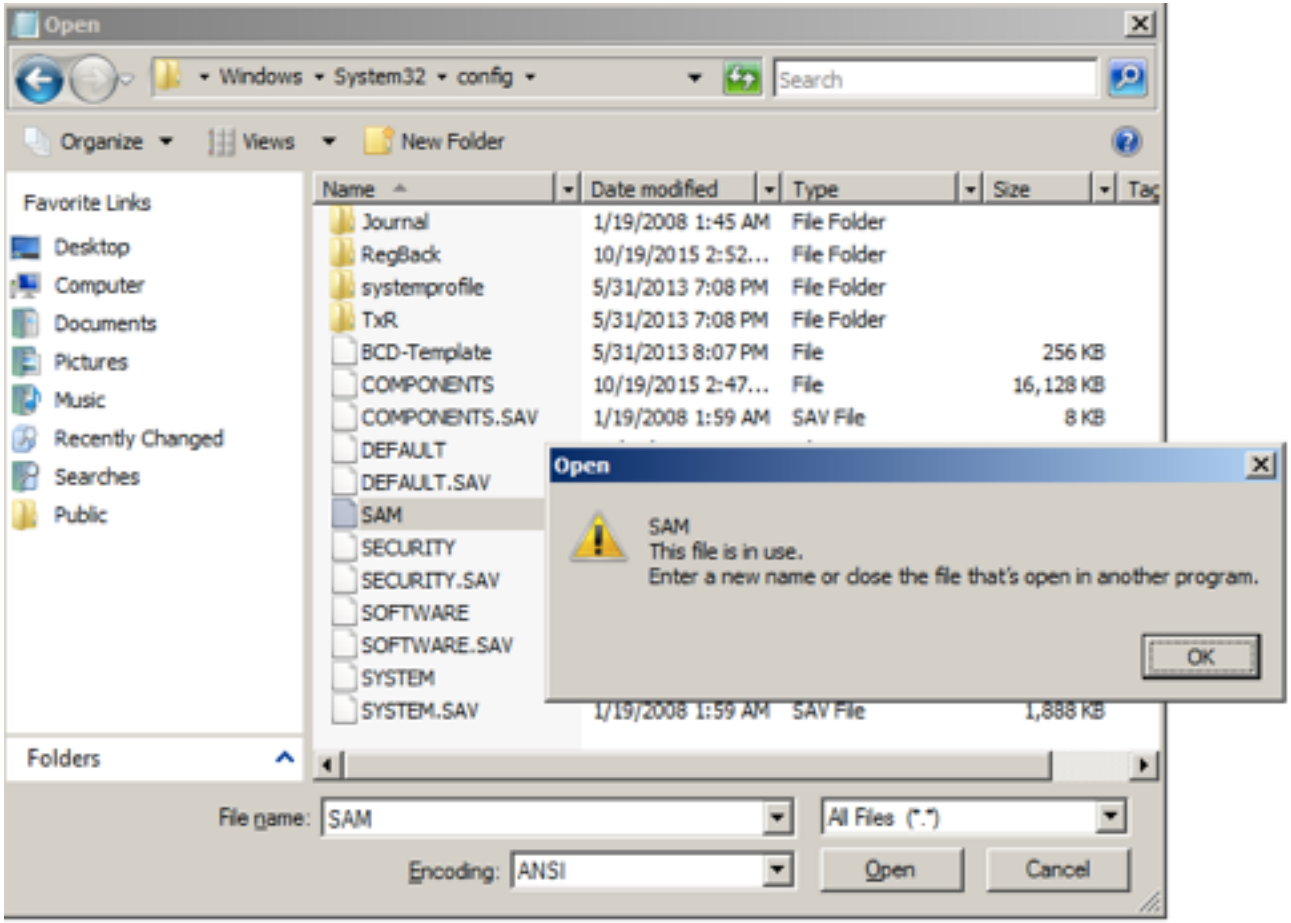
Two Ways to Strengthen Hashes

- 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

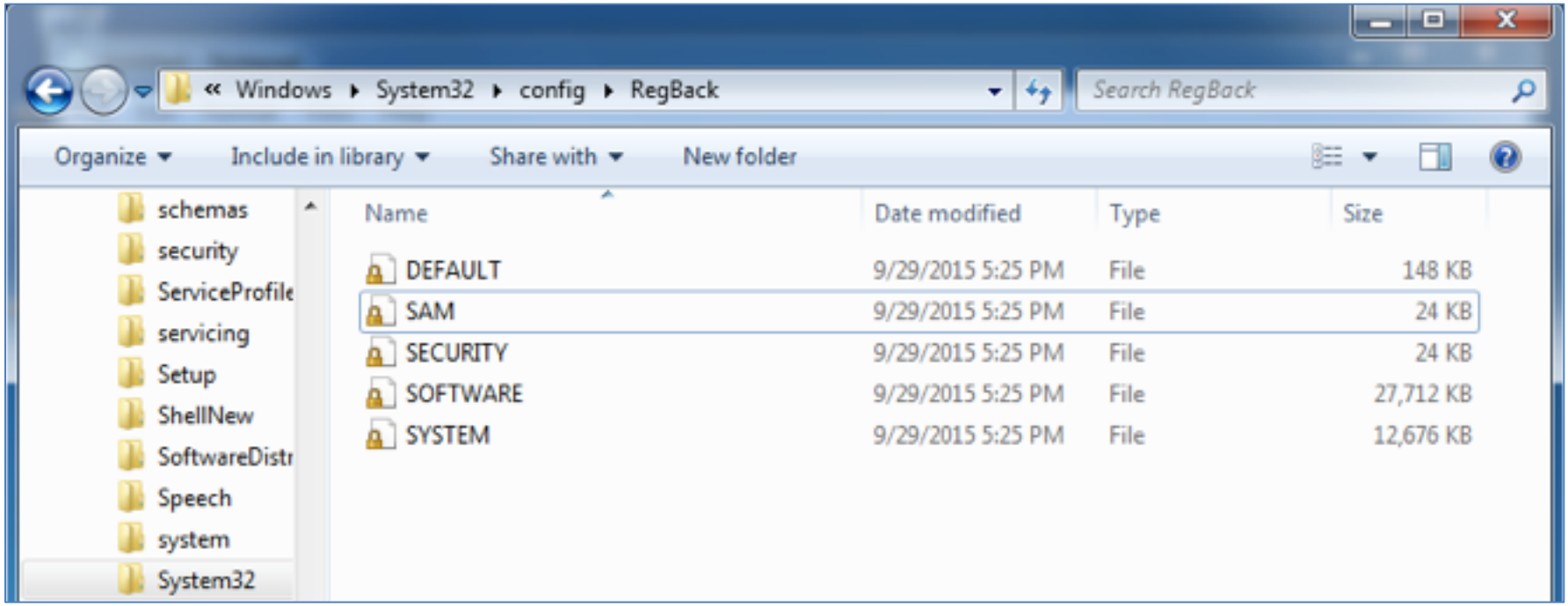


Unavailable when Windows is Running



Win 7 Backup Files

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



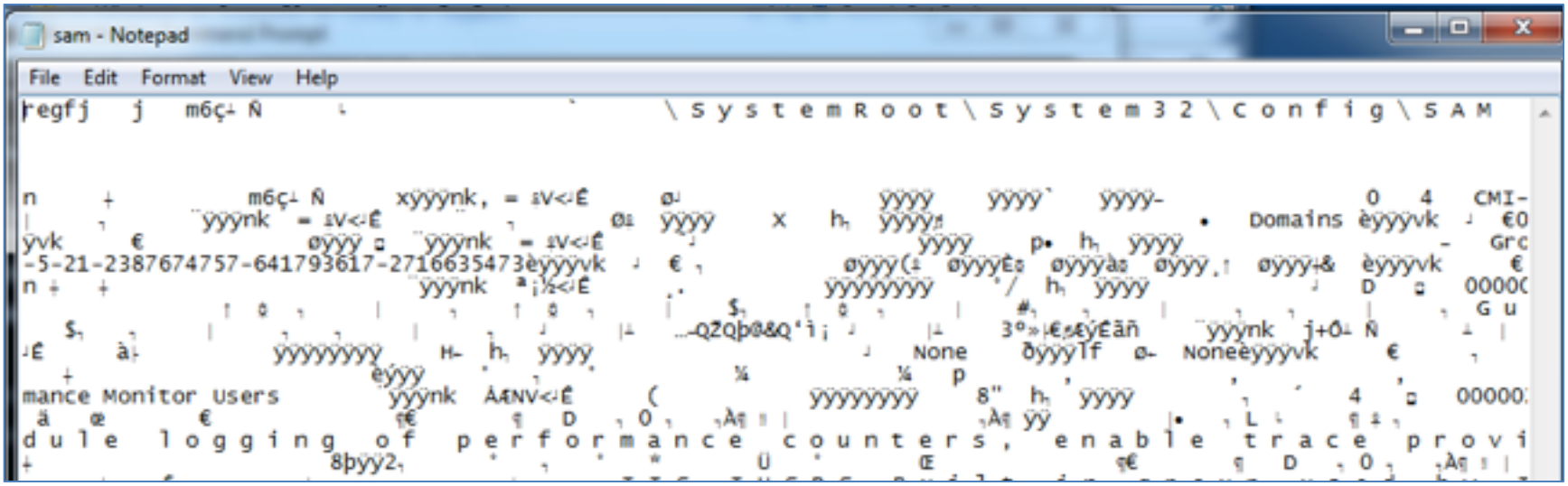
Reg.exe

- 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



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

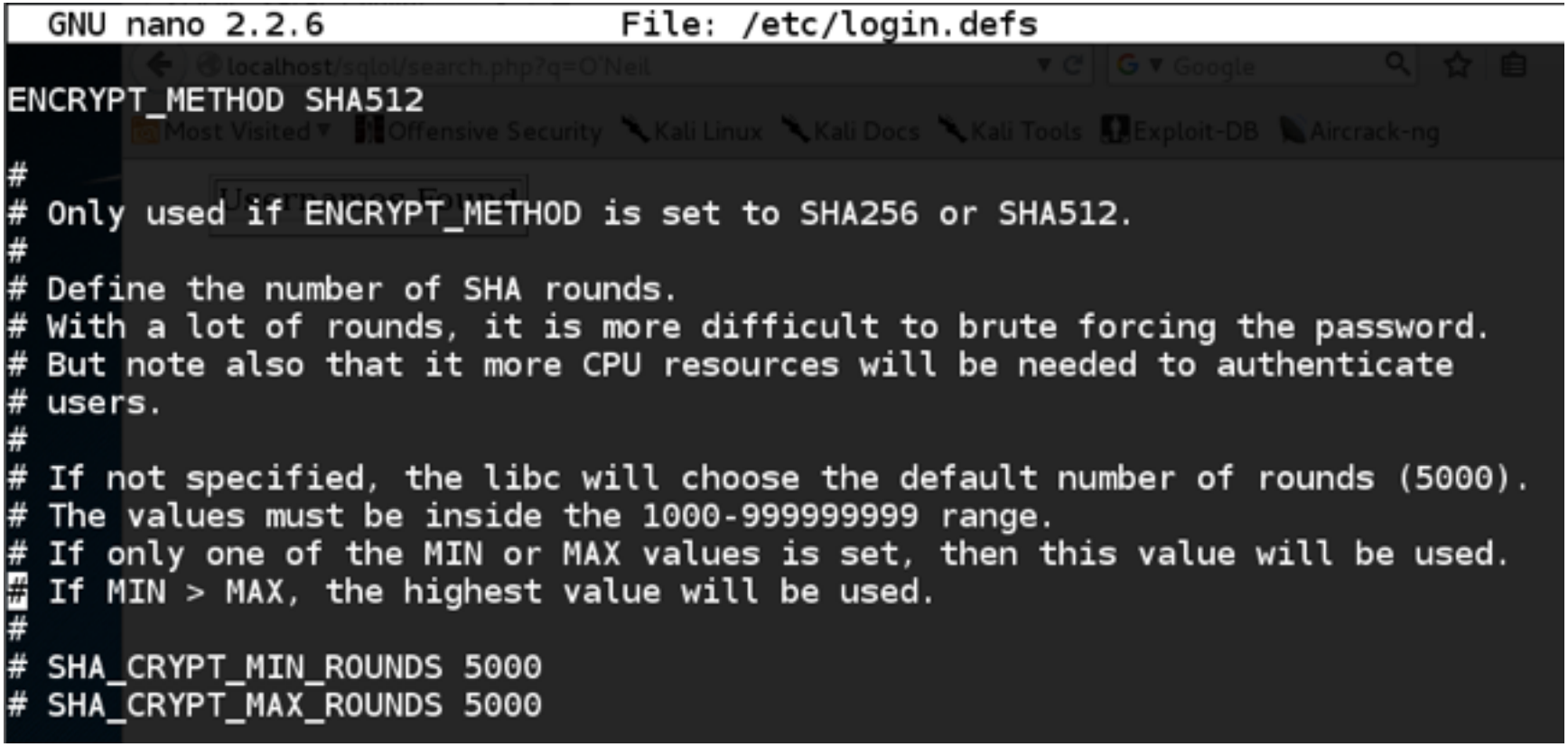
Cracking Windows Passwords

- 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



Cracking Kali Hashes

- Can only try 500 words in a few seconds

```
root@kali:~/124/ch9# cat /etc/shadow
root:$6$5bWGpZ9y$oDwaYKkWoXJoi0wClA7BoKwPW3DRaiUSZ4NI5McoZGLROwNeK.
IL0AxfgYZ61ME5OFQyXjP/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

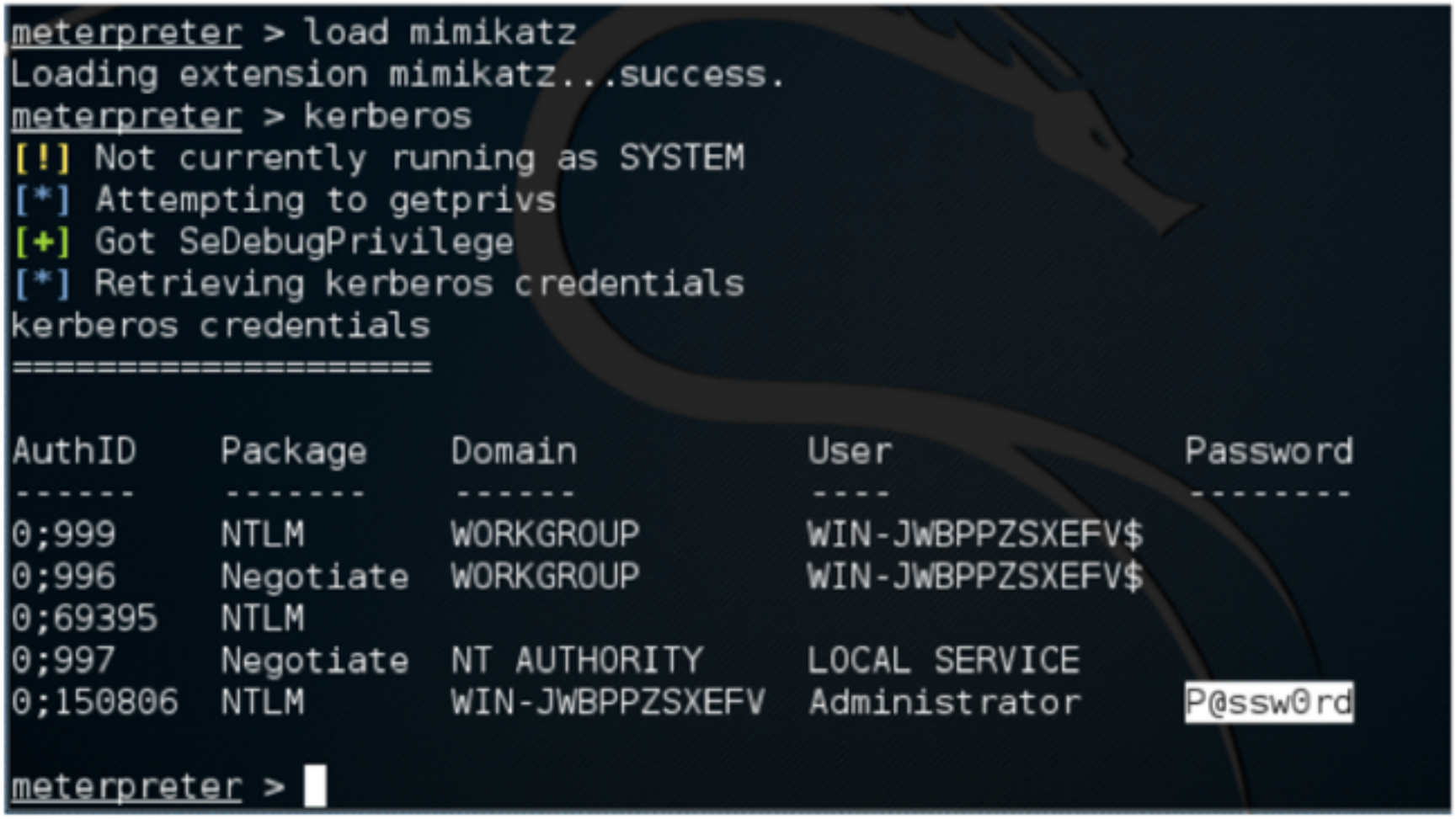
CloudCracker

- Moxie Marlinspike's service
- Runs on AWS machines

Cheap!


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

Mimikatz Gets Clear Passwords from RAM



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

Cracking 16 Character Strong passwords in less than an hour

Thursday, May 30, 2013 Mohit Kumar

- 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 "givemelibertyorgivemedeath" and other phrases.

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

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), "givemelibertyorgivemedeath" (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

pastebin.com/BuabHTvr

All aboard the Smoke & Flames Train. Last stop, Hell. You can have the pleasure of sharing seats with targets such as WallStreet, CIA Services, MIT, Consulting Firms, Political Advisors, Security Companies, Corporations, Weapon's Dealers, Laboratories, Internet Hosting Services, Academics, Banks, Police Departments, Aviation, The Navy, Stocks Exchange, Bonds Exchange, Markets, Emirates Organizations, Various Businesses, Hedge Funds, Estate Agencies, Public Affairs, Robotics, etc.

Team GhostShell's final form of protest this summer against the banks, politicians and for all the fallen hackers this year. With the help of it's sub-divisions, MidasBank & the newest branch, OphiusLab. One million accounts/records leaked. We are also letting everyone know that more releases, collaborations with Anonymous and other, plus two more projects are still scheduled for this fall and winter. It's only the beginning.

To conclude this summer's hacking spree, I will be giving away to anyone who's up for the challenge three different access points to three different groups/crews out there. It's our way of saying how great it's been raiding with you and let's hope that it isn't over just yet. The access-points are the following: 1. Six billion databases from a chinese mainframe full of chinese & japanese technology. It's very possible that it has from other countries as well, we haven't checked them all for obvious reasons. 2. Over 105 billion databases to a US stockexchange mainframe/s. It's very possible that the actual number is over 1 trillion, I wasn't prepared the first time and it gave me a memory error after 105 when it tried to add another digit. This job will require you to have at least 1TB available. 3. Access-points to 3-4 different servers belonging to the Department of Homeland Security. The sensitive information isn't that great but it may be good for street cred.

pastebin.com/BuabHTvr

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

---

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

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

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

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

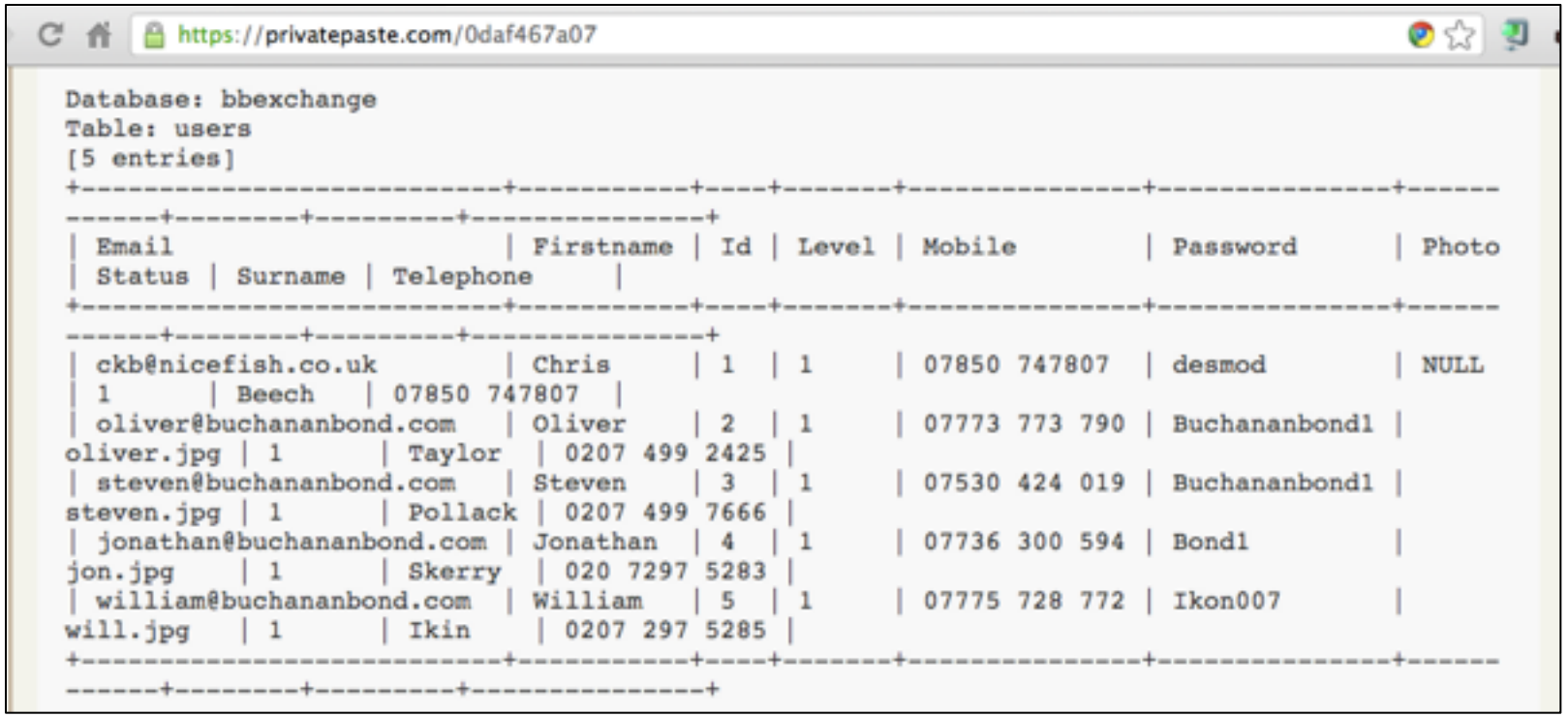
CIA Services Part5 - Mirror1 http://ideone.com/rswyv Mirror2 http://pastehtml.com/view/c9dy1fzp8.txt Mirror3 https://pastee.org/wptfx Mirror4 http://safebin.net/8221 Mirror5 https://gist.github.com/8b0803c5ac0c03791f98 Mirror6 http://pastesite.com/42282

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

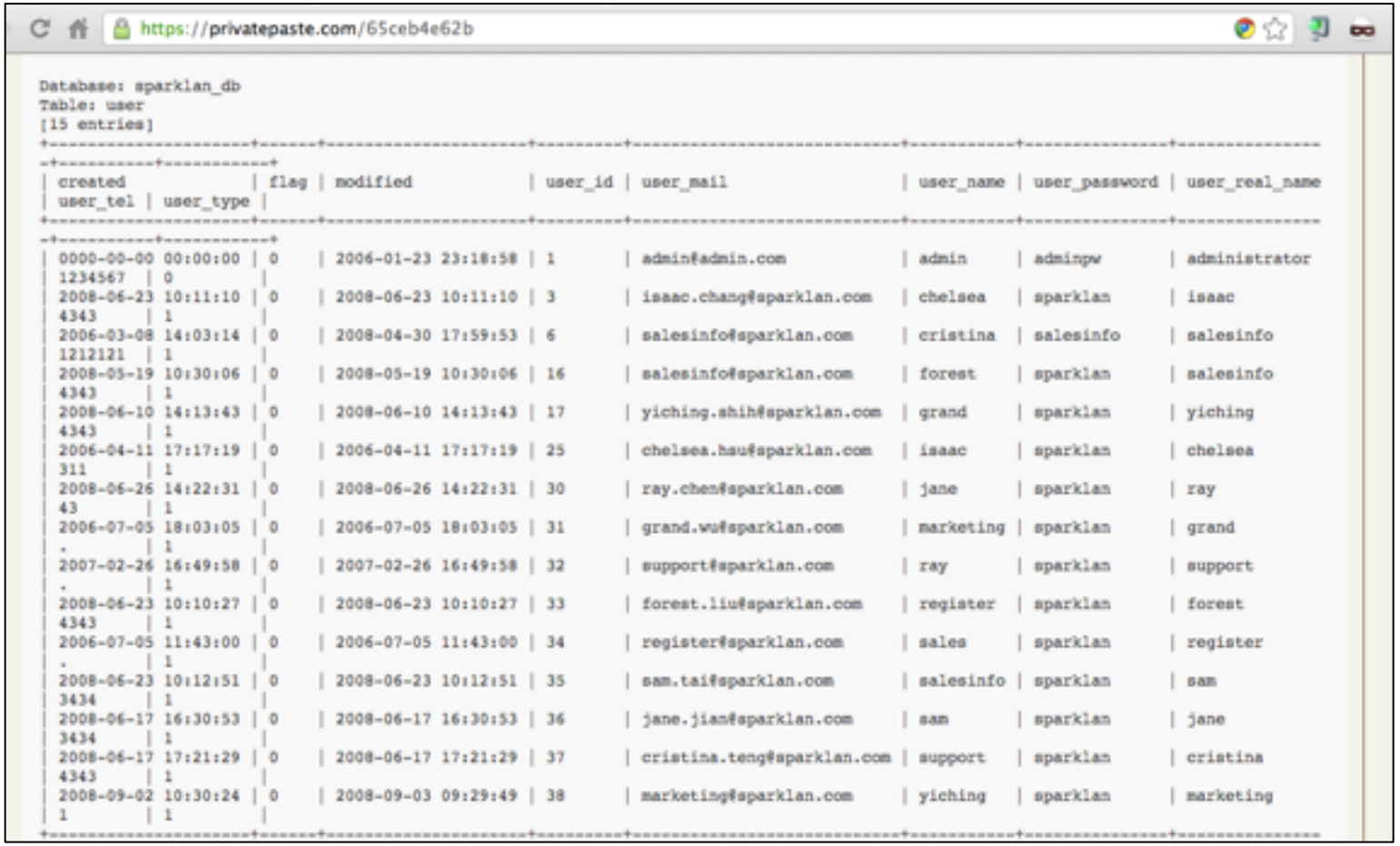
Plaintext Passwords, Easily Guessed



pastesite.com/42306

password	pay	position	username
1jlaw321	0	2	Lorraine
dllaw321	0	2	David
1234	0	2	Christy
jjlaw321	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	Erlie
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

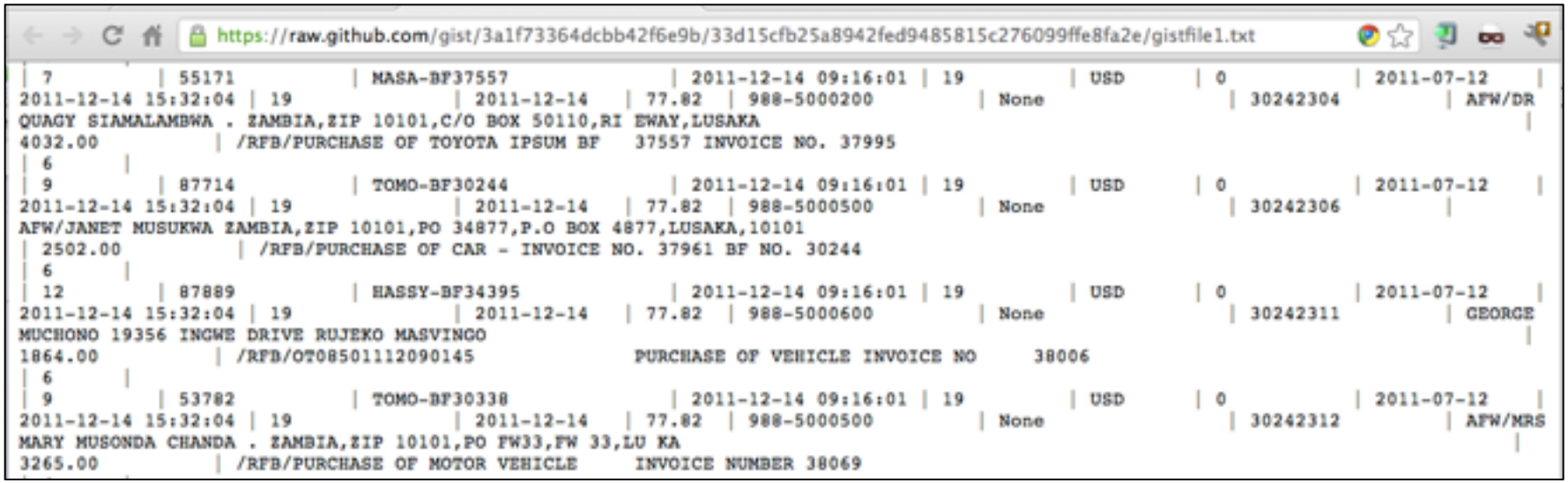


https://privatepaste.com/65ceb4e62b

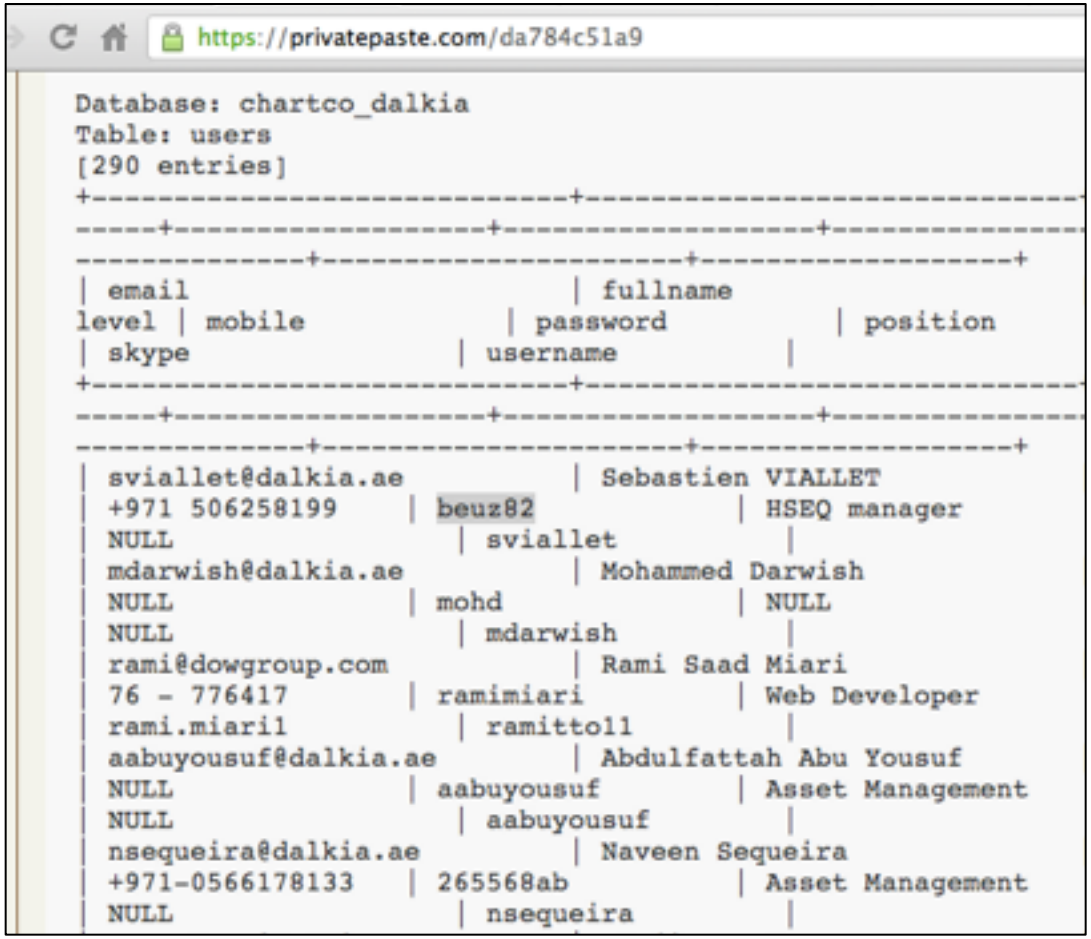
Database: sparklan_db
Table: user
[15 entries]

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

Beforward Transactions with PII



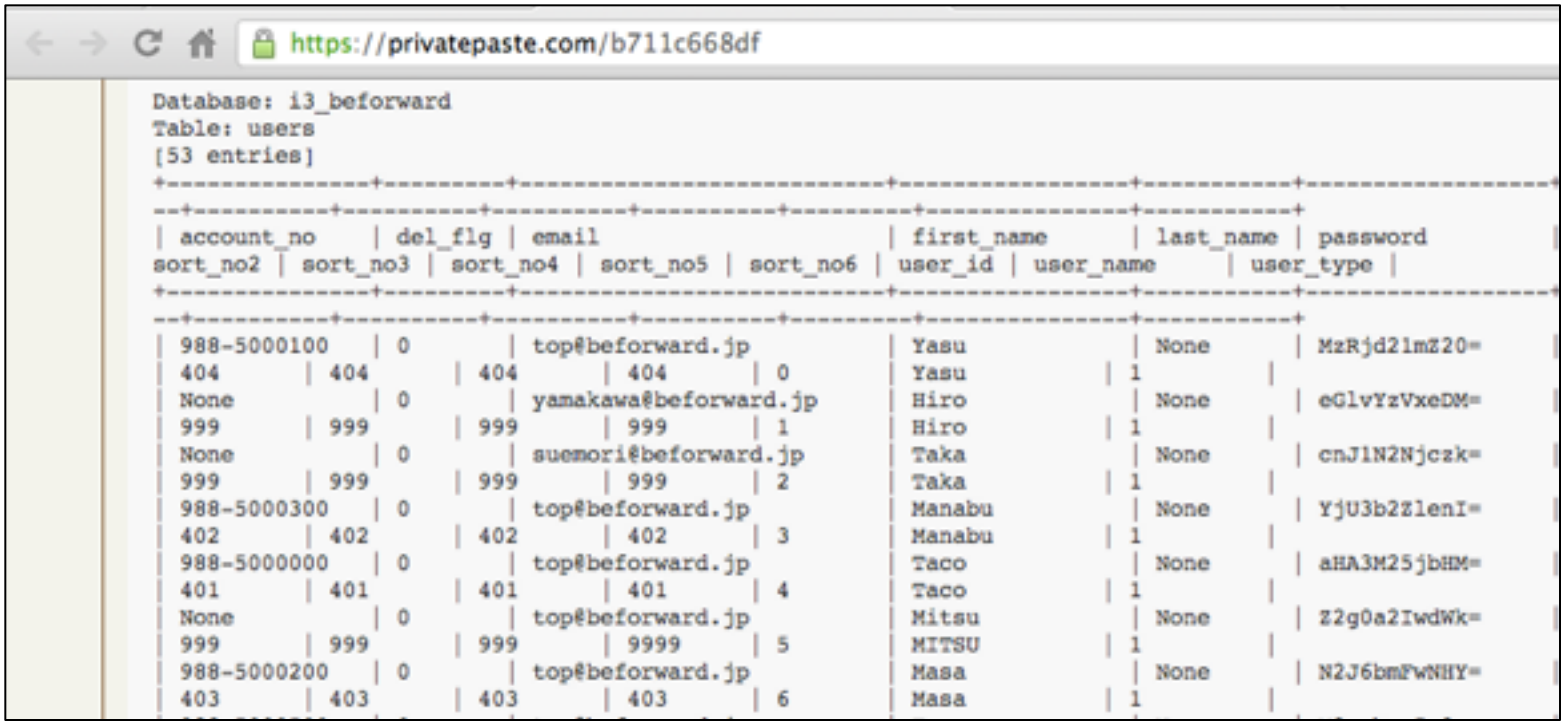
Plaintext Passwords



Password Storage: BASE64

Obfuscated, not hashed

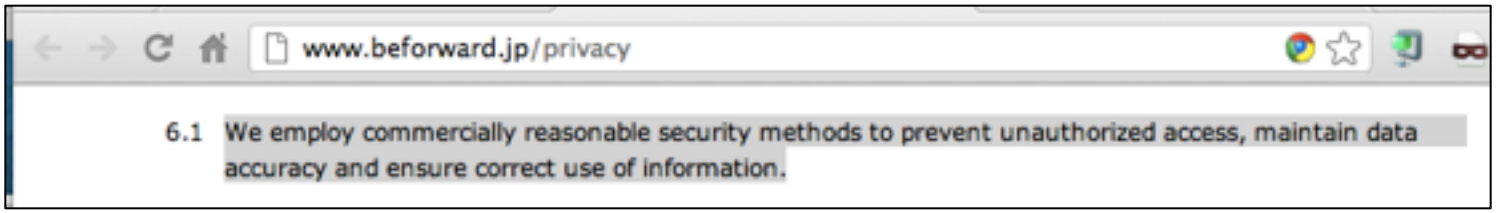
Beforward.jp



https://privatepaste.com/b711c668df

Database: i3_beforward
Table: users
[53 entries]

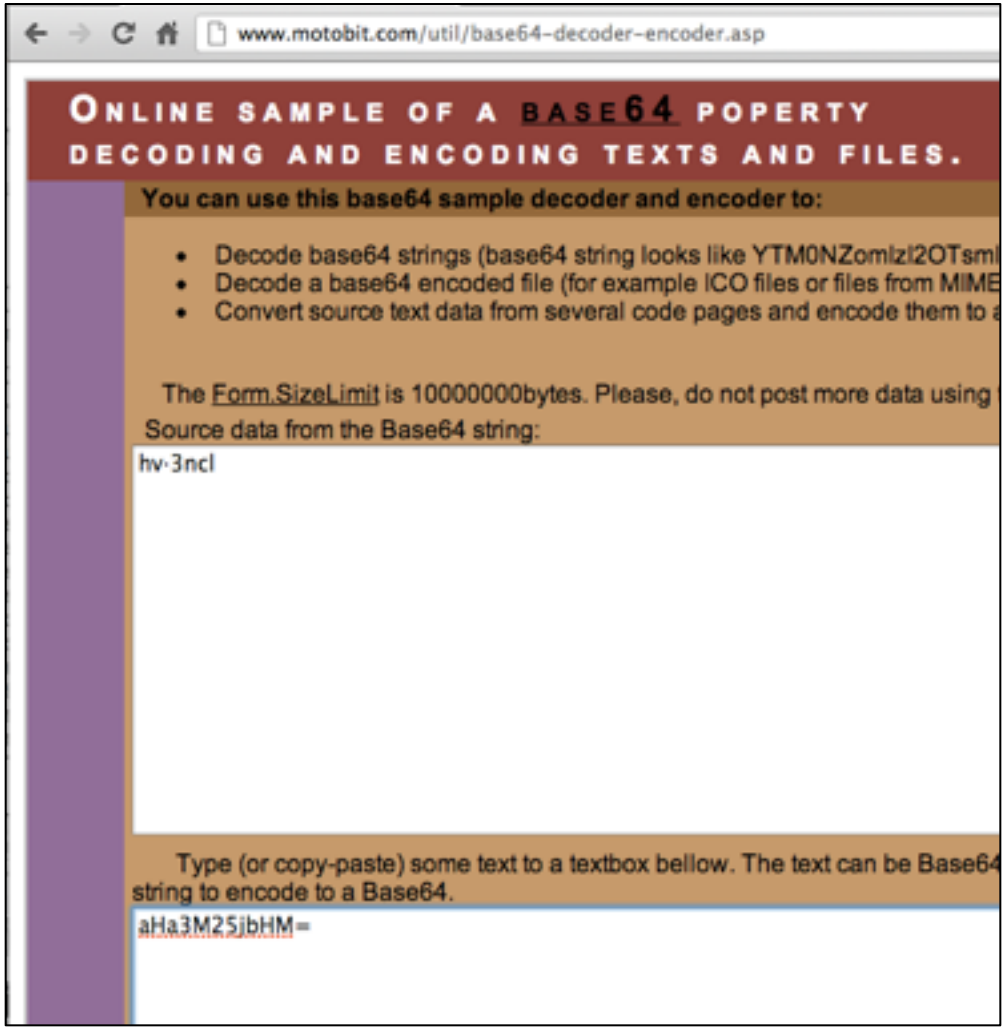
account_no	del_flg	email	first_name	last_name	password	sort_no2	sort_no3	sort_no4	sort_no5	sort_no6	user_id	user_name	user_type
988-5000100	0	top@beforward.jp	Yasu	None	MzRjd21mZ20=	404	404	404	404	0	Yasu	1	
None	0	yamakawa@beforward.jp	Hiro	None	eGlvYzVxeDM=	999	999	999	999	1	Hiro	1	
None	0	suemori@beforward.jp	Taka	None	cnJ1N2Njczk=	999	999	999	999	2	Taka	1	
988-5000300	0	top@beforward.jp	Manabu	None	YjU3b2ZlenI=	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	



www.beforward.jp/privacy

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

BASE64 Encoding



Password Storage: Unsalted MD5 or SHA-1

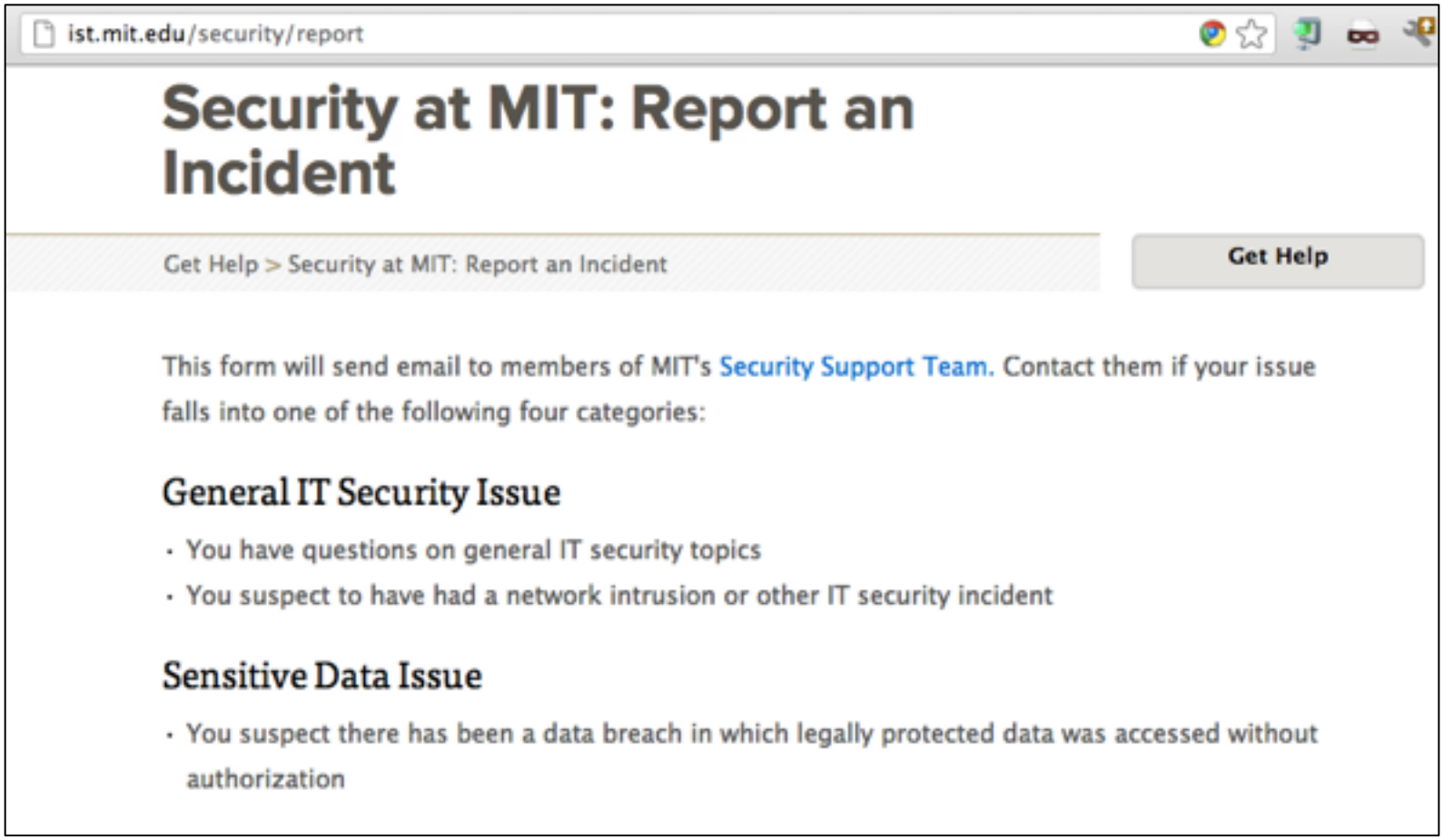
Real hashing, but very easy to crack

MIT – MD5 Password Hashes

safebin.net/8222

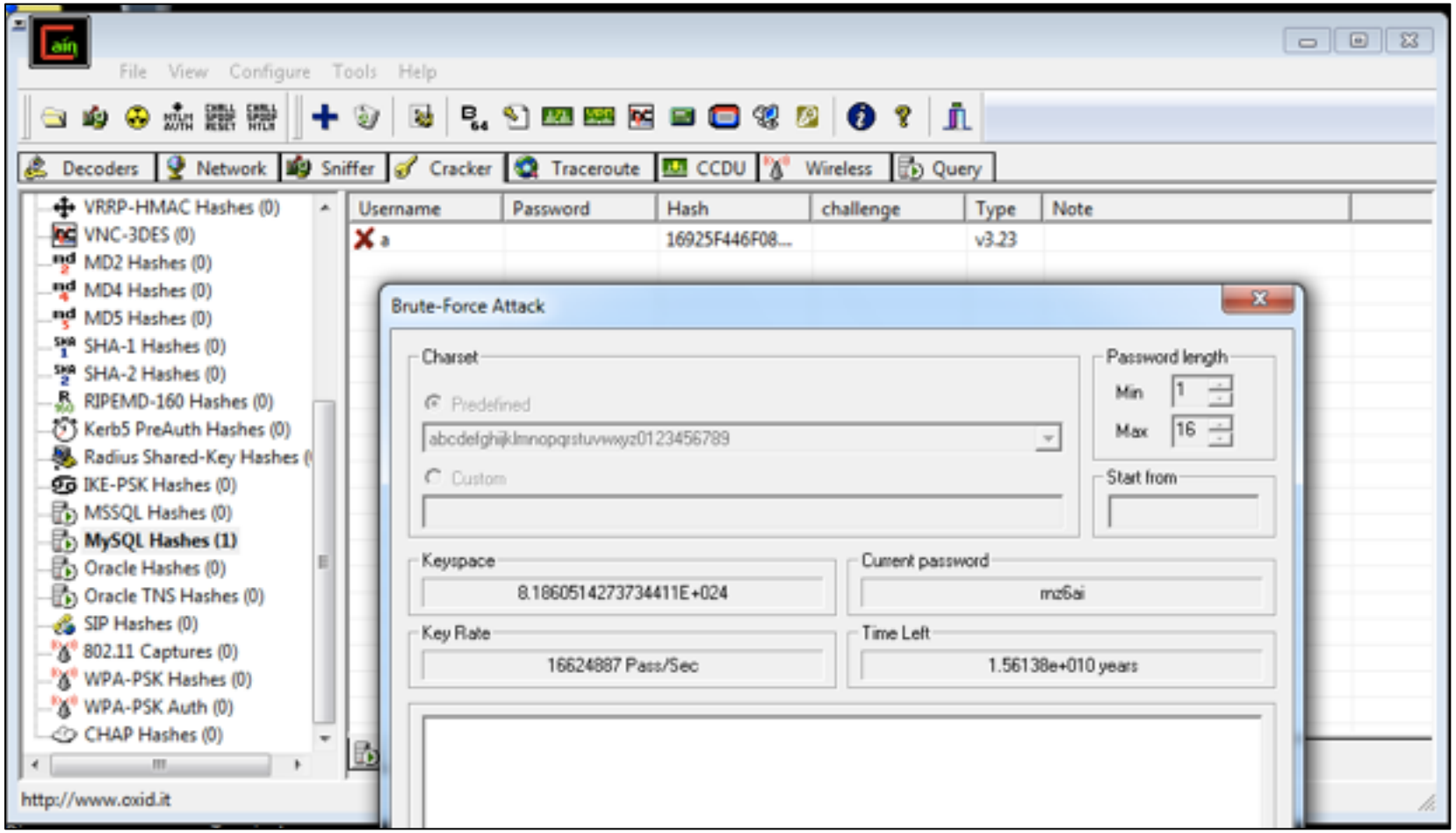
```
Database: materials
Table: tbl_mit_modul_users
[26 entries]
+------------------------------------------+---------------------+
| password                                 | username            |
+------------------------------------------+---------------------+
| 15ec04b902a94abb0abdc7c3455a9082         | rkemper@mit.edu     |
| 8d066a766c3991bee2dcfef1847d7b36         | jlandry@mit.edu     |
| ac404c90f9952be32e7ac004ff977cf9         | lmayer@MIT.EDU      |
| fff83b933071d358c88149f9a0f4d21d         | aglietti@MIT.EDU    |
| 9b656fa115a1e5b9f41f1f98a5727a92         | rsa@MIT.EDU         |
| 0c76f3625b9987550b0aae5325a3e904         | mtim@MIT.EDU        |
| 417e7aad3b19791275bb97399ff853ee         | pboisver@MIT.EDU    |
| ce0816e26302c5335f2158fc5f99142c         | yzhang05@MIT.EDU    |
| 4875dc668efbcb7f92b1b48b2b336481         | speakman@MIT.EDU    |
| c30fde34d9759760c4f0b6599fd58692         | sc79@MIT.EDU        |
| 90a3e0e7af307cf631ec83fc06b63800 (hiawatha) | elshaw@MIT.EDU      |
| f37a811c53a8b7656ac79a39e09efd39         | mbeals@MIT.EDU      |
| 437cf0b95453e22c351e2e031e0778d1         | tatem@MIT.EDU       |
| 87260b4fff690434a0f91d63511f98bc         | diadiuk@MIT.EDU     |
| 7f13daaf54c875ae01193401e76743b0         | mondol@nano.mit.edu |
| 5239ccd2aaca371c13118d1705647b48         | gpetrich@MIT.EDU    |
| 7b03d3bd7c900a377a8a6d0c113bf52b         | alan_s@MIT.EDU      |
| 8873d423e54e527201d03e3176d47d9b         | krystyn@MIT.EDU     |
| 37c9279d3fe9a0ae55f50874f1dedf0a         | watson@wi.mit.edu   |
| c5a1e49a6ead8b95eb84129cc2360663         | sdalton@MIT.EDU     |
| 90a242d8e9f077e03ae9b9e9c2d1fa10         | gedik@MIT.EDU       |
| 2cdcde61ccddabdec5342e7d72849819         | strano@mit.du       |
| 512a85775a359512123675f9c36de535         | pjarillo@MIT.EDU    |
| a7fed65ed81dc7bb821a43791afabbae         | asphodel@MIT.EDU    |
| a1354c3049f22725d7b07ddccf7f146d         | t_gray@MIT.EDU      |
| ea80e7b94d9077c0cdf28a001e41996b         | mpearrow@MIT.EDU    |
+------------------------------------------+---------------------+
```


www.md5decrypter.co.uk
MD5Decrypter.co.uk
IRC: irc.freenode.net
Channel: #md5decrypter
Use SSL, (Secure Socket Layer)
eck 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.
How many decryptions are in your database?
We have a total of just over 8.7 billion unique decrypted MD5 hashes since August 2007.
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.
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
ac404c90f9952be32e7ac004ff977cf9 MD5: vorg7r5a
Please note the password is after the : character, and the MD5 hash is before it.
Decrypt Hashes
abc123
Load new captcha


ist.mit.edu/security/report
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

Cracking Hashes with Cain



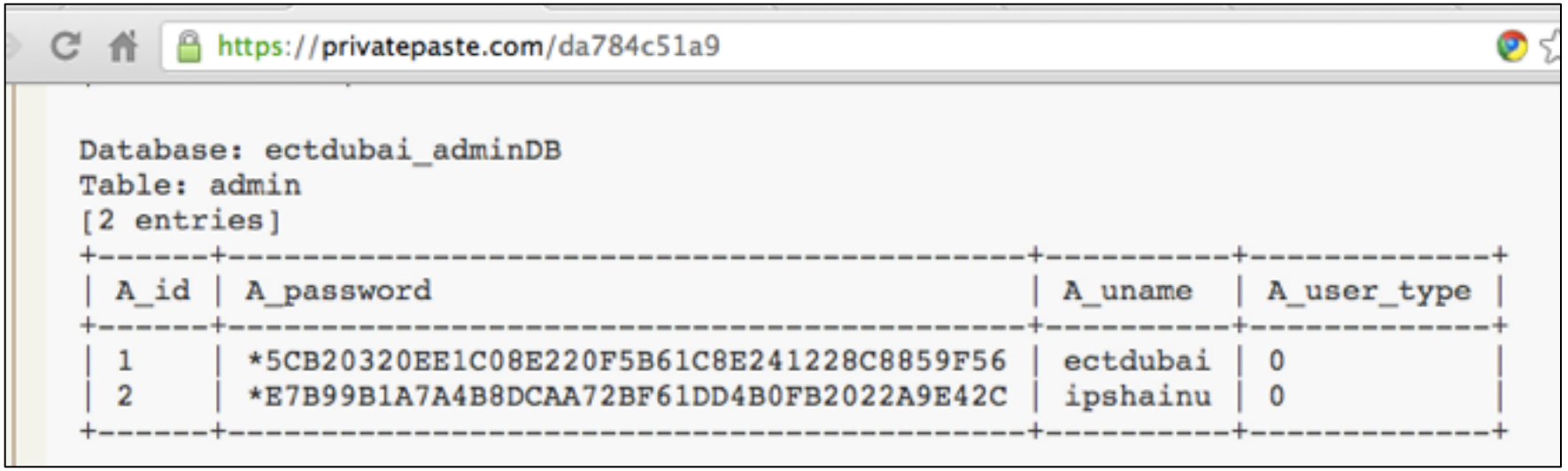
SHA-1 Hash


https://privatepaste.com/da784c51a9
Database: industri_web
Table: members
[1 entry]
| email | name | password |
| industrial | Admin User | e6ae401ee24a014f691bc260fe77b62e03be0e1d |

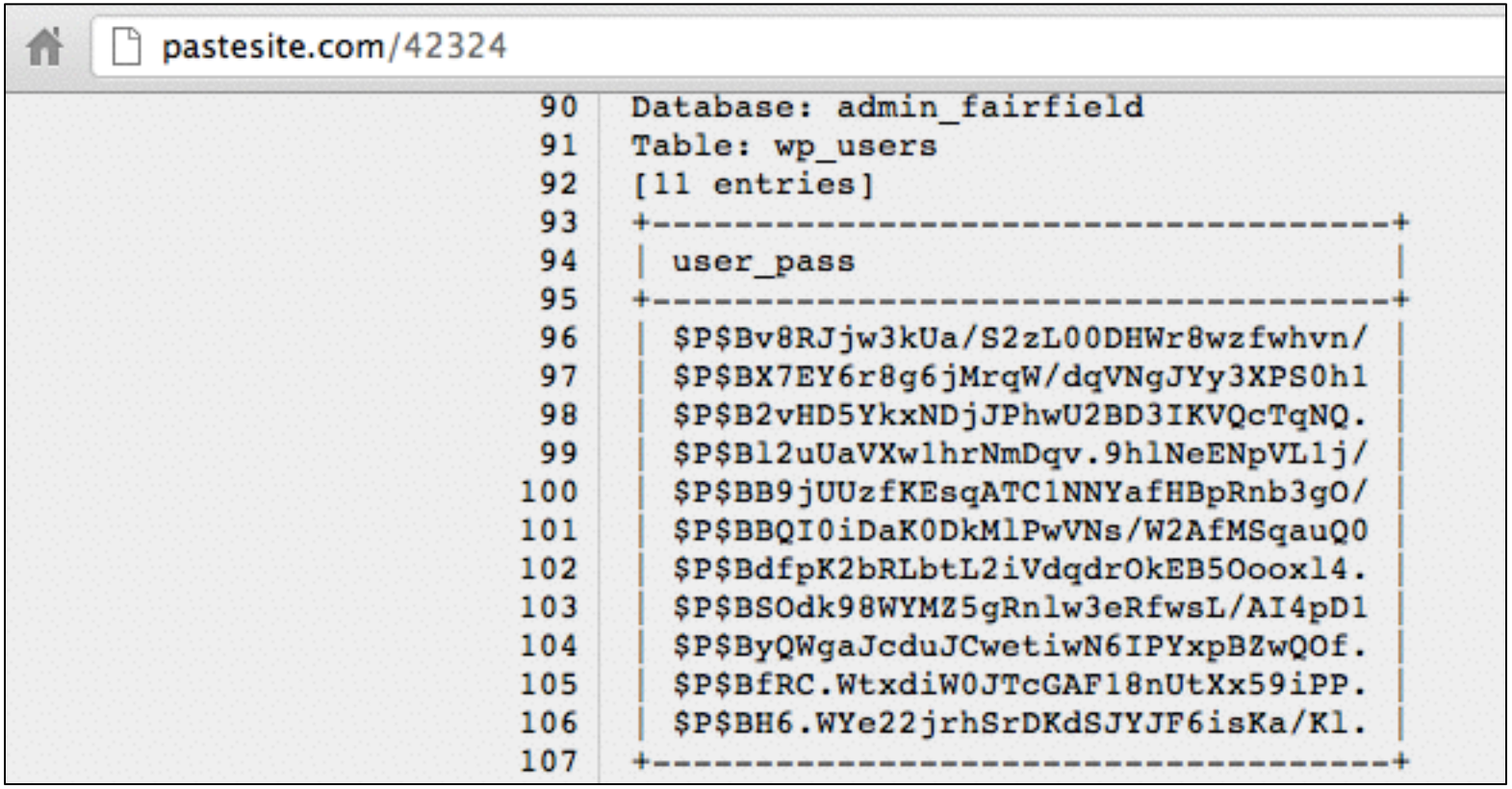
Cracked!


www.md5decrypter.co.uk/sha1-decrypt.aspx
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
What does this SHA1 / MySQL Decrypter tool do?
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.
How many decryptions are in your database?
We have a total of just over 8.7 billion unique decrypted SHA1 hashes since December 2009.
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.
Please input the SHA1 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...
SHA1 Hashes:
Max: 16
Please use a standard list format
e6ae401ee24a014f691bc260fe77b62e03be0e1d
e6ae401ee24a014f691bc260fe77b62e03be0e1d SHA1: ben24690740

MySQL 5 Password Hashes

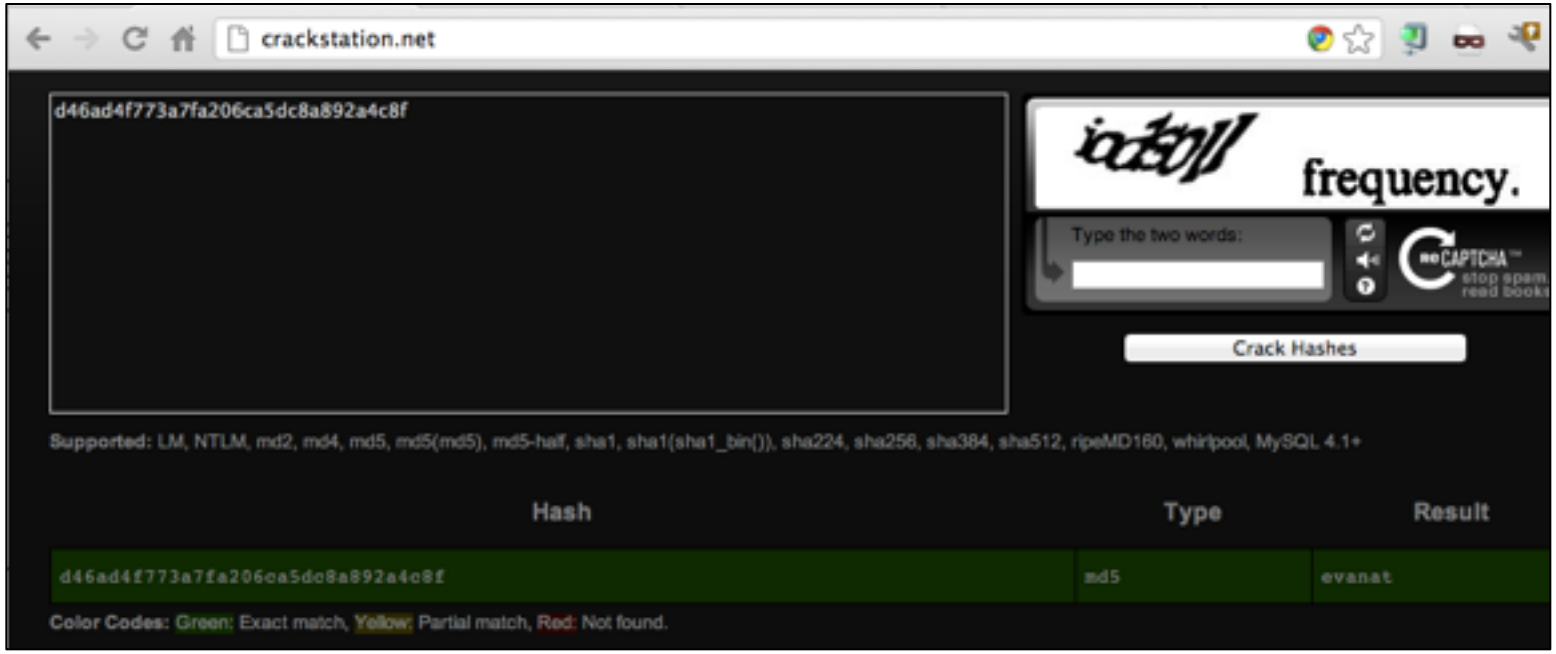


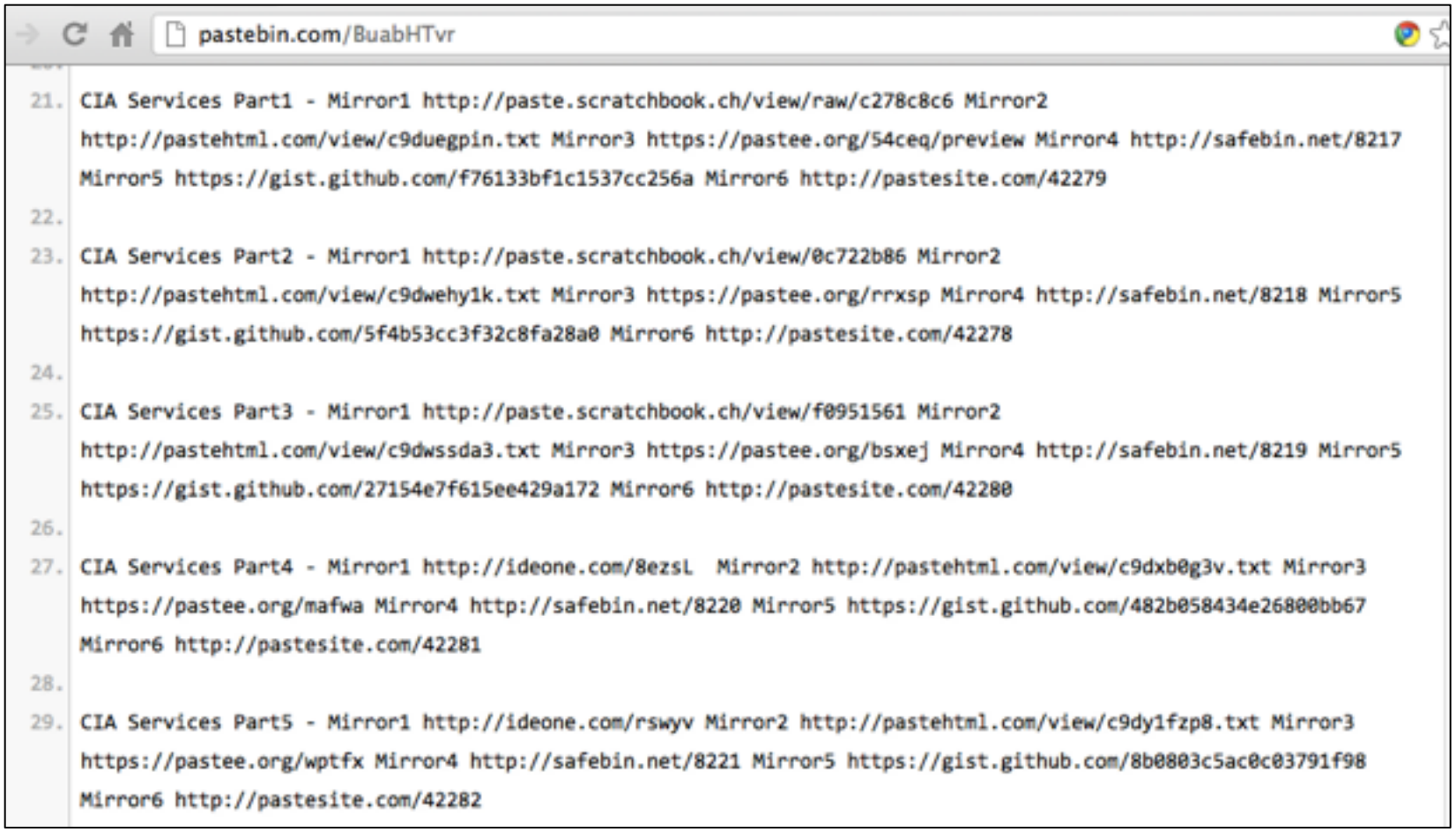
Wordpress Password Hashes

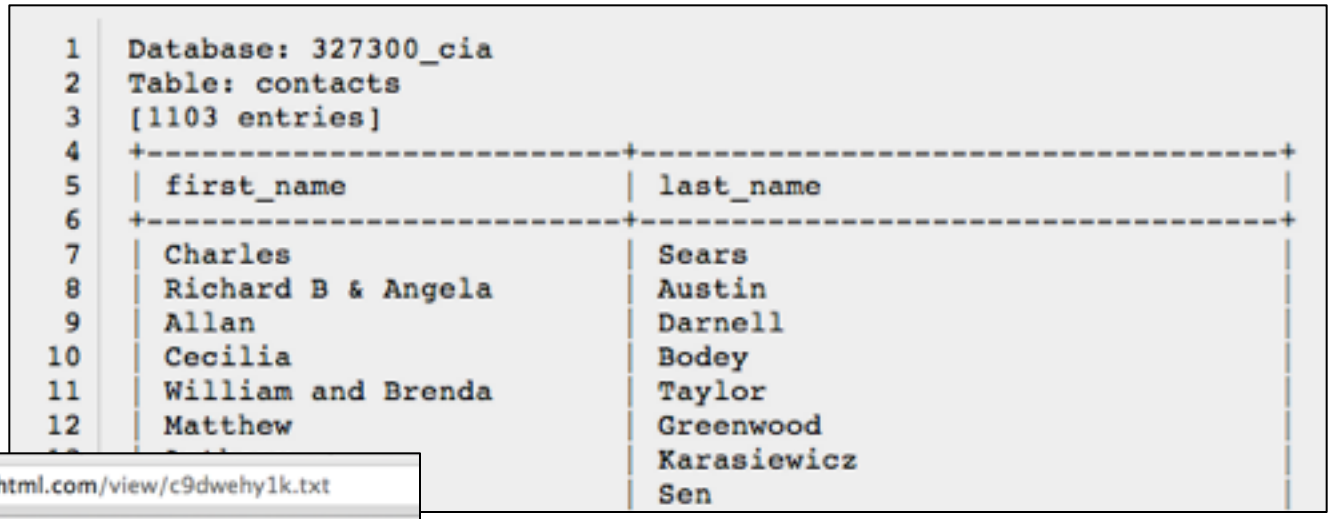


Relative Space

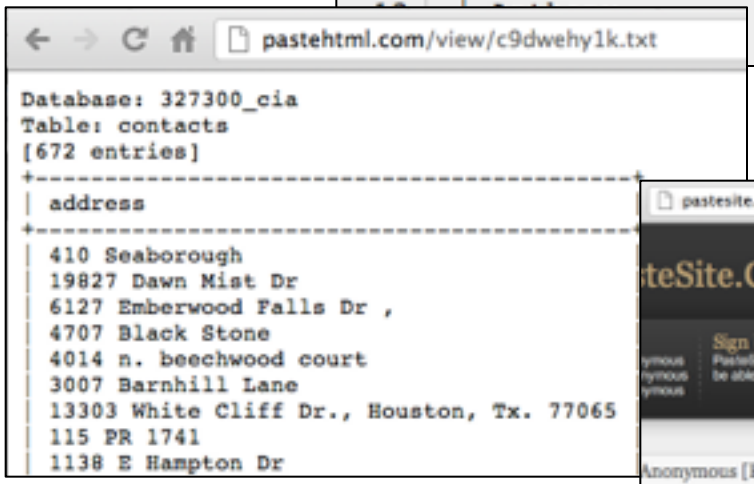
Cracked!


crackstation.net
d46ad4f773a7fa206ca5dc8a892a4c8f
frequency.
Type the two words:
reCAPTCHA
stop spam.
read books
Crack Hashes
Supported: LM, NTLM, md2, md4, md5, md5(md5), md5-half, sha1, sha1(sha1_bin()), sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+
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

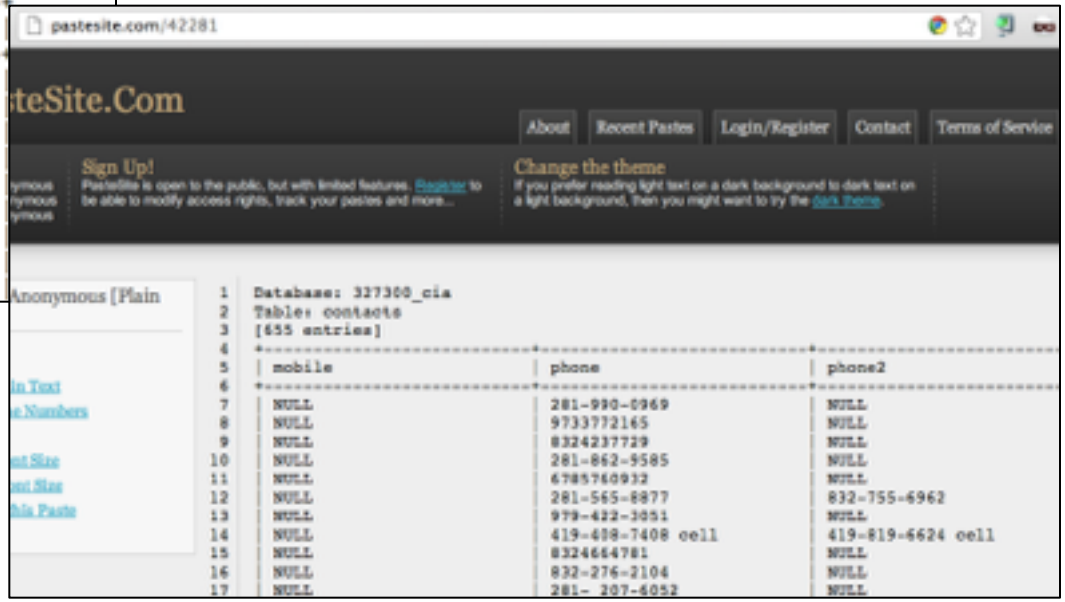


```
Database: 327300_cia
Table: contacts
[1103 entries]
+--------------------------+-------------------------------------+
| first_name               | last_name                           |
+--------------------------+-------------------------------------+
| Charles                  | Sears                               |
| Richard B & Angela       | Austin                              |
| Allan                    | Darnell                             |
| Cecilia                  | Bodey                               |
| William and Brenda       | Taylor                              |
| Matthew                  | Greenwood                           |
|                          | Karasiewicz                         |
|                          | 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!

Change the theme

Anonymous [Plain

```
Database: 327300_cia
Table: contacts
[655 entries]
+-----------------------+-----------------------+-----------------------+
| mobile                | phone                 | phone2                |
+-----------------------+-----------------------+-----------------------+
| NULL                  | 281-990-0969          | NULL                  |
| NULL                  | 9733772165            | NULL                  |
| NULL                  | 8324237729            | NULL                  |
| NULL                  | 281-862-9585          | NULL                  |
| NULL                  | 6785760932            | NULL                  |
| NULL                  | 281-565-8877          | 832-755-6962          |
| NULL                  | 979-422-3051          | NULL                  |
| NULL                  | 419-488-7408 cell     | 419-819-6624 cell     |
| NULL                  | 8324664781            | NULL                  |
| NULL                  | 832-276-2104          | NULL                  |
| NULL                  | 281- 207-6052         | NULL                  |
```

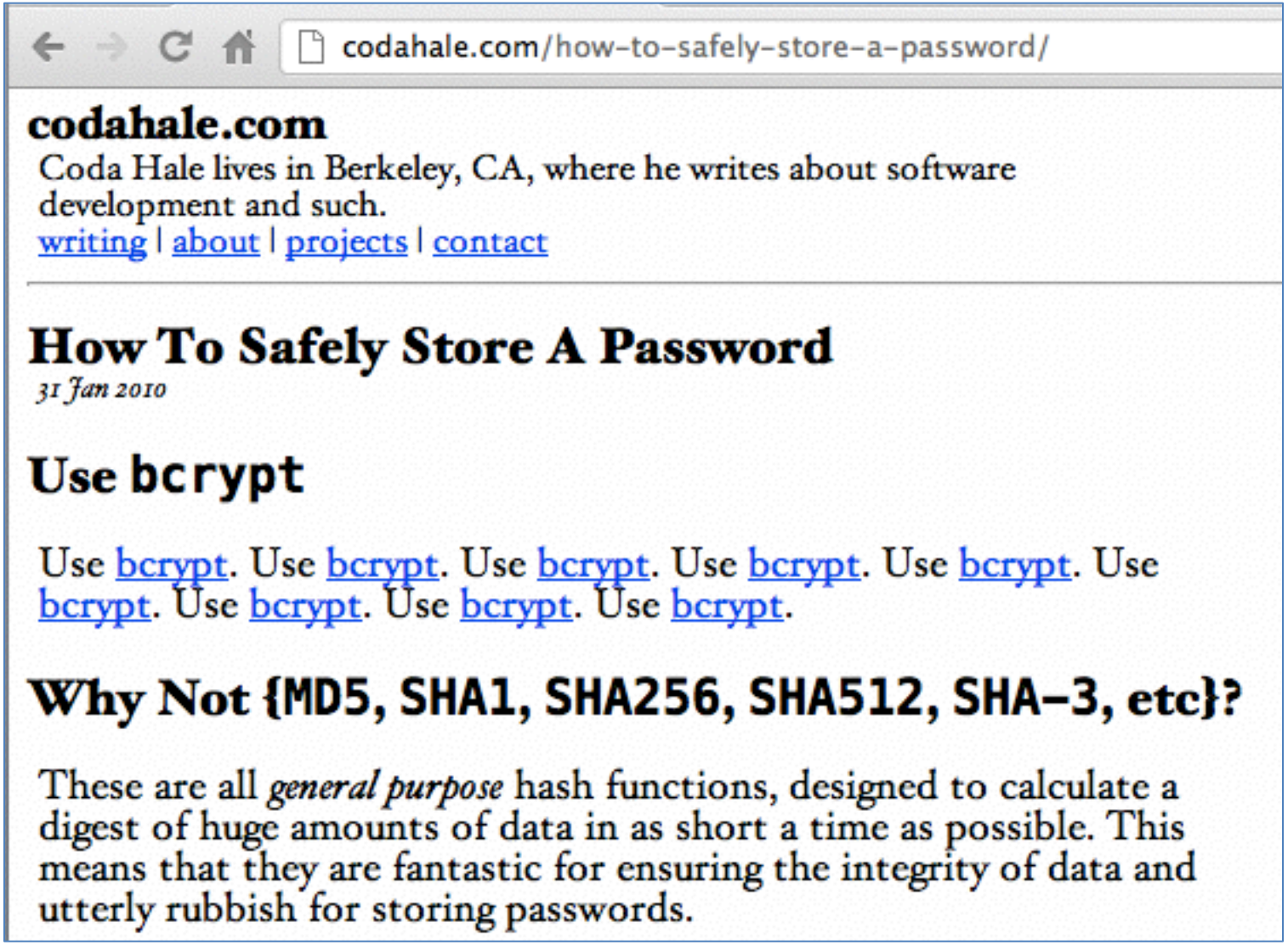
Password Hashing Algorithms

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


www.101hacker.com/2010/12/hashes-and-seeds-know-basics.html
HOME ABOUT US CONTACT US ADVERTISE WRITE FOR US
HACKAHOLIC
Ethical hacking | Cybersecurity
Home Products Contents BlogRoll
EMULATORS DOWNLOADS TOOLS
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



codahale.com/how-to-safely-store-a-password/

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