GUIDEBOOK

decrypter RELEASE

Fitur Inside :

1. **Cryptography With Subtitution Method**
2. **Encoding base64**
3. **Decoding base64**
4. **Hash-identifier**
5. **Findmyhash Cracking MD5 | MD4 | SHA1 | SHA-256**
6. **MD5 Generator**
7. **MD4 Generator**
8. **SHA1 Generator**
9. **SHA-256 Generator**
10. **Qrcode**
11. **Keyloger With Xspy**

Visit : www.xsanlahci.wordpress.com

report bug :   xsanlahci[at]gmail.com

IBTeam
REVOLUTION

xsan-lahci

Contents

1. Introduction of dEcrypt3r V2

Now dEcrypt3r has been release on Version 2.
This script is under GPL v3 License (http://www.gnu.org/licenses/gpl-3.0.html).
Copyright (c) 2013 xsan-lahci aka Vaisal Dot Zip | Fuck For PLAGIARISM
DISCLAIMER: modifications, changes, or alterations to this sourcecode is acceptable, however, any public releases utilizing this code must be approved by writen this tool (xsan-lahci)
Report Bugs : xsanlahci[at]gmail.com | xsan[at]idblackhat.org
Thanks for your nice ideas and help to make this tool more useful:
Mr.Iqbal a.k.a Ikonspirasi | Zion3R (hash-id) | laXmarcaellugar (findmyhash) | Kentaro Fukuchi (qrencode) | JAM (xspy)
Greetz to : http://www.indonesianbacktrack.or.id | http://www.idblackhat.org and | http://forum.blacknewbieteam.org
dont forget to visit my BLog http://xsanlahci.wordpress.com
Follow me : @vaisal_exe > Like my FP : facebook.com/XsanLahci
Special Thanks To: My God Allah.SWT | My Parents | My Teacher | My Sister And My Love Nabila And Many Thanks For my Friends @ University and Facebook

1.1 Cryptography Subtitution Method

What is Cryptography Subtitution Method?
We know many tricks about cryptography,and subtitution method is a basic
cryptography,the basic method is make table , for example

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
B	F	1	K	Q	G	A	T	P	J	6	H	Y	D	2	X	5	M	V	7

U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0			
C	8	4	1	9	N	R	E	U	3	L	S	W	,	.	0			

if the cipher text "INDONESIA" and we want to encrypt this word,after encrypt word
"INDONESIA" to be "PDK2DQVPB" and we want back to decrypt this word, after
decrypt "PDK2DQVPB" , we have chiper text "INDONESIA".But in dEcrypt3r V2 i
use special character inside,like character from russian language,japan,korean language .
So Attacker cannot decrypt message if he not use dEcrypt3r.

1.2 Encrypt Message With dEcrypt3r

example : choose 1 for Encrypt your message

look the Picture !
The Chiper text is : Studying Indonesian Language
We got The encrypt Message to be : кkD>GWuQ|5u>Tu?SW:u|2:uQD:Q?

1.3 Decrypt Message With dEcrypt3r

example : choose 2 for Decrypt your Message

Look The Picture!
The Encrypt Text is : кkD>GWuQ|5u>Tu?SW:u|2:uQD:Q?
We got chiper text after decrypt : Studying Indonesian Language

2. Encoding & Decoding Base 64

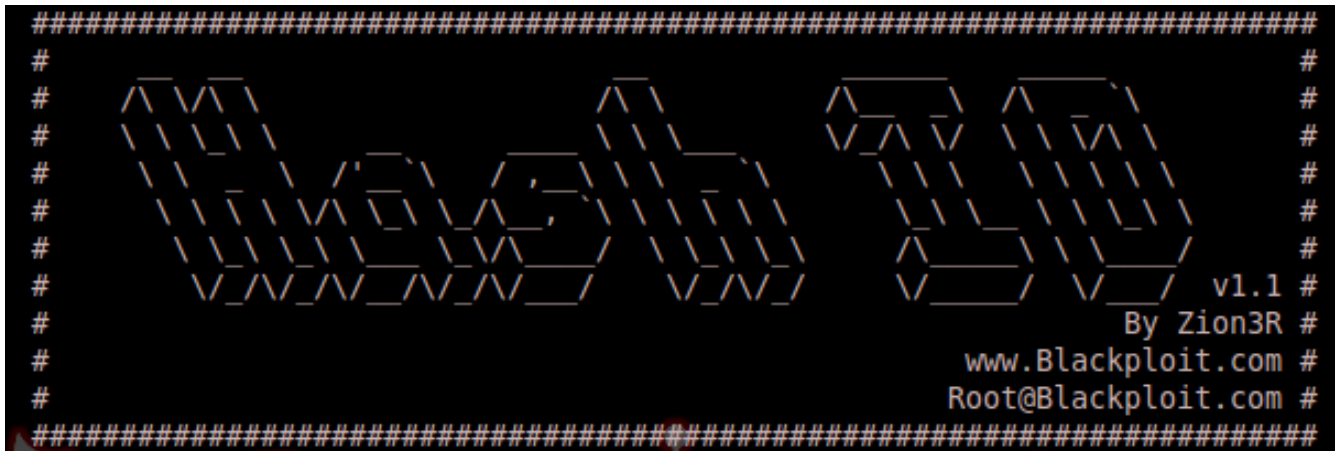## 2.1   Encoding base64 With dEcrypt3r :

2.2   Decoding base64 With dEcrypt3r :

```
Select Menu   :
          1) choose 1 for encrypt your message
          2) choose 2 for decrypt your message
          3) choose 3 for Encoding base64
          4) choose 4 for Decoding base64
          5) choose 5 for Hash-identifier
          6) choose 6 for findmyhash Cracking MD5
          7) choose 7 for findmyhash Cracking MD4
          8) choose 8 for findmyhash Cracking SHA1
          9) choose 9 for findmyhash Cracking SHA-256
         10) choose 10 for MD5 Generator
         11) choose 11 for MD4 Generator
         12) choose 12 for SHA1 Generator
         13) choose 13 for SHA-256 Generator
         14) choose 14 for qrcode
         15) choose 15 for Keyloger With Xspy
         99) choose 99 for Credits and About
         00) choose 00 for Exit
dEcrypt3r:>4
insert your message for decoding base64:ZEVjcnlwdDNyLVYuMgo=
your message after decoding base64 is:dEcrypt3r-V.2
```

3. Hash Identifier

```
###################################################################
#                                                                 #
#      __    __                      __                 ___   ___  #
#     /\ \  /\ \                    /\ \               /\___\/\___\ #
#     \ \ \ \ \ \      __      ____ \ \ \___           \/___/\/___/ #
#      \ \ \ \ \ \   /'__`\   /',__\ \ \  _ `\            __   __   #
#       \ \ \_\ \ \ /\ \L\.\_/\__, `\ \ \ \ \ \          /\_\ /\_\  #
#        \ \_____\ \\ \__/.\_\/\____/  \ \_\ \_\         \/_/ \/_/  #
#         \/_____/\/_/\/__/\/_/\/___/   \/_/\/_/            v1.1    #
#                                                        By Zion3R #
#                                                www.Blackploit.com #
#                                               Root@Blackploit.com #
#                                                                 #
###################################################################
```

Hash Id is tool for identification any hash , not for cracking hash, this is tool coded by Zion3R, I think this is powerfull tool for identification hash example detected hash :

- **MD5**
- **MD4**
- **MD5 Wordpress**
- **Salt**
- **SHA1**
- **SHA256**
- **DES(Unix)**
- **and many more**

3.1   Hash-id With dEcrypt3r

Example : choose 5 for Hash ID

HASH : ZiY8YtDKXJwYQ
Possible Hashs:
[+] DES(Unix)

4. Findmyhash

Findmyhash is hash online cracking tool.coded by laXmarcaellugar, more info? Lets try
root@linux:~# ./findmyhash -h
./findmyhash.py 1.1.2 (http://code.google.com/p/findmyhash/)
Usage:
------
 python ./findmyhash.py \<algorithm> OPTIONS
Accepted algorithms are:

  MD4   - RFC 1320
  MD5   - RFC 1321
  SHA1   - RFC 3174 (FIPS 180-3)
  SHA224   - RFC 3874 (FIPS 180-3)
  SHA256   - FIPS 180-3
  SHA384   - FIPS 180-3
  SHA512   - FIPS 180-3
  RMD160   - RFC 2857
  GOST   - RFC 5831
  WHIRLPOOL - ISO/IEC 10118-3:2004
  LM   - Microsoft Windows hash
  NTLM   - Microsoft Windows hash
  MYSQL   - MySQL 3, 4, 5 hash
  CISCO7   - Cisco IOS type 7 encrypted passwords
  JUNIPER - Juniper Networks 9 encrypted passwords
  LDAP_MD5 - MD5 Base64 encoded
  LDAP_SHA1 - SHA1 Base64 encoded
 Examples:

  -> Try to crack only one hash.
     python ./findmyhash.py MD5 -h 098f6bcd4621d373cade4e832627b4f6

  -> Try to crack a JUNIPER encrypted password escaping special characters.
     python ./findmyhash.py JUNIPER -h "\$9\$LbHX-wg4Z"

  -> If the hash cannot be cracked, it will be searched in Google.
     python ./findmyhash.py LDAP_SHA1 -h "{SHA}cRDtpNCeBiql5KOQsKVyrA0sAiA=" -g

  -> Try to crack multiple hashes using a file (one hash per line).
     python ./findmyhash.py MYSQL -f mysqlhashesfile.txt

     Contact:

[Web]   http://laxmarcaellugar.blogspot.com/
[Mail/Google+] bloglaxmarcaellugar@gmail.com
[twitter]   @laXmarcaellugar

4.1 Cracking MD5 With findmyhash on dEcrypt3r

example :

Look The Picture

Insert your md5 : d911d1bcff2ef5fd896c07450ab2f997

And wait for the second.. until this tool finish scanning your Hash md5

4.2   Cracking MD4 With findmyhash on dEcrypt3r

example :

your Hash md4 is : db346d691d7acc4dc2625db19f9e3f52

***** HASH CRACKED!! *****

The original string is: test

The following hashes were cracked:

db346d691d7acc4dc2625db19f9e3f52 -> test

4.3   Cracking SHA1 With findmyhash on dEcrypt3r

example : choose 8

Look the picture
your SHA1 :e272b04b0f79fc5068a3646ec8d052e9cf0fa7f8

**** HASH CRACKED!! *****
The original string is: test123$

The following hashes were cracked:
----

e272b04b0f79fc5068a3646ec8d052e9cf0fa7f8 -> test123$

4.4   Cracking SHA-256 With findmyhash on dEcrypt3r

example : choose 9

your SHA-256 :
03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4

Cracking hash:
03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4

Analyzing with askcheck (http://askcheck.com)...

***** HASH CRACKED!! *****
The original string is: 1234

The following hashes were cracked:

03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4 -> 1234

5.   Multiple Hash Generator

5.1   MD5 Generator with dEcrypt3r
example : choose 10

insert your message!: dEcrypt3r.V2
your md5 is: ecb09595b0668363f581dadd81b48157

done :D

5.2   MD4 Generator with dEcrypt3r
example : choose 11

your message!: test
your md4 is: db346d691d7acc4dc2625db19f9e3f52

Finish :D

5.3 SHA1 Generator with dEcrypt3r
example : choose 12

your message!: dEcrypt3r by xsan-lahci
your SHA1 is: fead3307f794978de59a009712b499c607e3d3f8

5.4 SHA-256 Generator with dEcrypt3r
example : choose 13

your message!:1234
your SHA-256 is:03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4

6.   Qrcode with Qrencode on dEcrypt3r

Qrencode is Application for make Qrcode,this tool coded by Kentaro Fukuchi for more info , you need install this tool .
root@linux:~# apt-get install qrencode
root@linux:~# qrencode -h
Copyright (C) 2006, 2007, 2008 Kentaro Fukuchi
Usage: qrencode [OPTION]... [STRING]
Encode input data in a QR Code and save as a PNG image.

```
 -h           display this message.
 --help       display the usage of long options.
 -o FILENAME  write PNG image to FILENAME. If '-' is specified, the result
              will be output to standard output. If -S is given, structured
              symbols are written to FILENAME-01.png, FILENAME-02.png, ...;
              if specified, remove a trailing '.png' from FILENAME.
 -s NUMBER    specify the size of dot (pixel). (default=3)
 -l {LMQH}    specify error collectin level from L (lowest) to H (highest).
              (default=L)
 -v NUMBER    specify the version of the symbol. (default=auto)
 -m NUMBER    specify the width of margin. (default=4)
 -S           make structured symbols. Version must be specified.
 -k           assume that the input text contains kanji (shift-jis).
 -c           encode lower-case alphabet characters in 8-bit mode. (default)
 -i           ignore case distinctions and use only upper-case characters.
 -8           encode entire data in 8-bit mode. -k, -c and -i will be ignored.
 -V           display the version number and copyrights of the qrencode.
 [STRING]  input data. If it is not specified, data will be taken from
              standard input.
```

On dEcrypt3r.V2 is very simple and easy use lets check this out
example : choose 14

Enter a name for the output with 'example.png'
xsan.png
write text for qrcode
cryptography
check your directory! xsan.png finish

# 7.	Keyloger with Xspy on dEcrypt3r

Who dont know keyloger? For record any typing on your keyboard,xspy can record virtual keyboard on your LCD.How to use on dEcrypt3r.V2 ?Please check This out !

Example : choose 15

Wait your victim to type the word."ctrl+c" for Exit | check log.txt!

In Your Folder dEcrypt3r.V2 , log.txt and spy.rb has been added.. when you running keyloger,you just need the victim use your computer / your server and type many word

now check your log.txt!
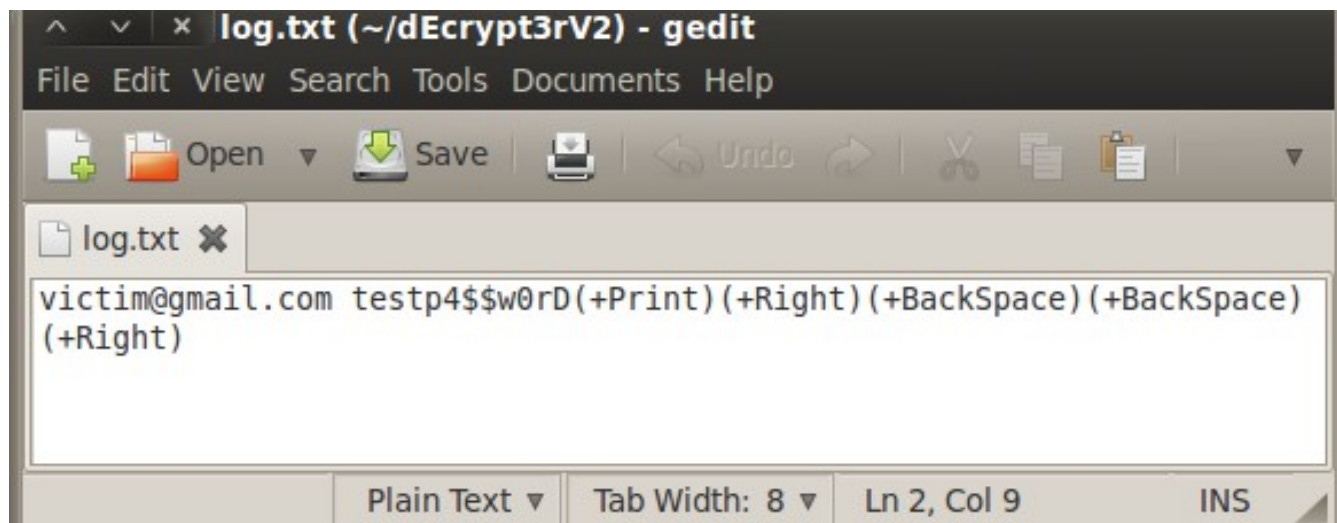
Look at the picture !

victim@gmail.com with password is testp4$$w0rD

| dEcrypt3r V.2 | Copyright 2013 | Xsan-Lahci | xsanlahci[at]gmail.com |

Thanks to all my friend on facebook and suport
special thanks to > My God Allah | My parents | My sister | and My Girlfriend
Special Thanks for your nice ideas and help to make this tool more useful:
Zee Eichel > You tell me about security and make me love bash programing
Mr.Prionggo > You are my best Teacher in University | my Teacher Criptograph
Ikonspirasi > Thanks For Your suport and many more :D
Zion3R   > Your Hash Identifier is Amazing and Cool
laXmarcaellugar > Your Findmyhash is very great and Amazing
Kentaro Fukuchi > Your qrencode is very nice
JAM   > Your xspy is very Powerfull
Thanks To All Member and Crew IBTeam | all member and Crew idblackhat
Thanks To All crew Blacknewbieteam | All Regional Indonesian Backtrack Team
Thanks For My Best Teacher and Best Friends : Jimmyromanticdevil | GTX150
JurankDankal | Shadowmaker | Nasa | Snail_v3n0m | Guitarisnoize | TheUndick |
devilnay | lasax | Mr.Iwan.S | james0baster | cassaprodigy | junior | shendo
 | dr.wine | sasaka | Alp0ah | gnome selpa | sanimorpix_tux | black dragon | U5hant |
koecroet | THJC | Andre_Corleone | mywisdom | iyansquid | computer_geex
zasad | larcenciels | ande ande lumut | minal texas | nanokbocahkidrock
madan | Arul zomb | abdee_dillah | drewc0de | nisan | 5forA | AresThehopebuster
cyberking | kakus130908 | alpoah | GTX150 | amstrong | mendskin | Arfha | cod3
Udalah | ardy | eigy | rendy | irpan | temon | turn off | joko | kambing |
kahfie hudson | Pak RT | Pak LUrah | PAkpolisi aka bangdevils | d3b14n | joejoen
Pak hansip | Kodoknjepatselalu | Monox | kiddies | Andynosetrave | civil kidz
black orion | MrBs | Adhitya_DCasterX-ID | m4k4s4rh4ck3r | nefrit | ekawithyou
Serbian Haxor CyberWorM | Steck > And ZQ@r From Madleets | cybernuxbie
inj3ct0r | Cupid sh3ll Bangladesh Blackhat Team | Hax0rlif3 Madleets crew | all my
friends .

Visit my forum   :
www.indonesianbacktrack.or.id
www.idblackhat.org
www.forum.blacknewbieteam.org
my blog   : www.xsanlahci.wordpress.com
my socialnetwork : facebook.com/XsanLahci | @vaisal_exe

About the Authors

Vaisal aka Xsan-Lahci I was Born on Jakarta 1992.Still studied at University in South Jakarta,I'm Admin Forum Indonesian Backtrack,Admin Forum Black Newbie Team and Moderator Forum Indonesian Blackhat Team / idblackhat.org
I'm Co Trainer at Codewall-Security.
Now I have made two applications for Linux
The First Application is Clear-Log , and the Second Application is dEcrypt3r,you can fine my Application at xsanlahci.wordpress.com/mytools/ , and i use Bash Programing. Please if you fine any bugs on my tools,send to my email

xsanlahci@gmail.com | xsan_lahci@indonesianbacktrack.or.id | xsan@idblackhat.org

dont forget to visit

www.indonesianbacktrack.or.id
www.blog.indonesianbacktrack.or.id
www.idblackhat.org
www.forum.blacknewbieteam.org
www.codewall-security.com
www.xsanlahci.wordpress.com
www.ikonspirasi.me