



Project 2

CTF

Antonin Vannier

Summary



Challenges

1

Cryptography - Unrecognized hash (Easy)

2

Cryptography - Secret message (Easy)

3

Steganography - Cats (Hard)

CTF 1 - Description

INSTRUCTIONS



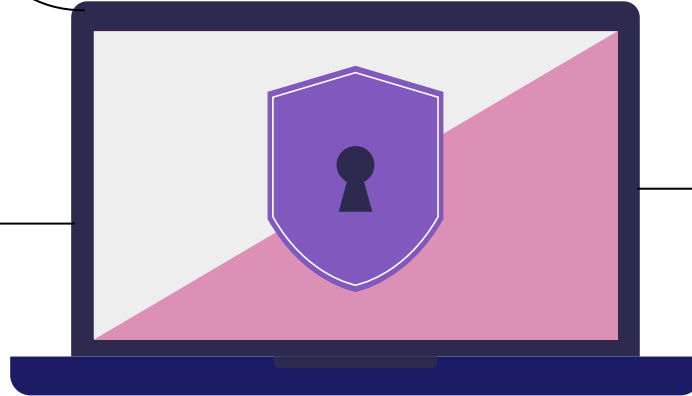
You are given a hash, but its format seems unknown. Find the corresponding uncracked password.

Documents



Zip containing :

- unknownhash.txt
- readme.txt
- challengevalidation.zip



HOW TO VALIDATE ?

Return the MD5 hash of the password

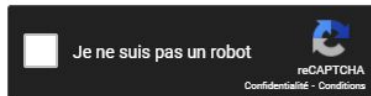
CTF 1 - Resolution

```
kali@kali:~/Documents/CTF/crypto$ cat unknownhash.txt
7b5c96484h6f1daaa2611dea7e82f34ea87005ee04a659935d38e367fea900bb3
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

7b5c96484h6f1daaa2611dea7e82f34ea87005ee04a659935d38e367fea900bb3



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
7b5c96484h6f1daaa2611dea7e82f34ea87005ee04a659935d38e367fea900bb3	Unknown	Unrecognized hash format.

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

Check the length of the hash !

Known hash functions



CTF 1 - Resolution

```
kali@kali:~/Documents/CTF/crypto$ cat unknownhash.txt  
7b5c96484h6f1daaa2611dea7e82f34ea87005ee04a659935d38e367fea900bb3
```

→ 65 digits



CTF 2 - Description

INSTRUCTIONS



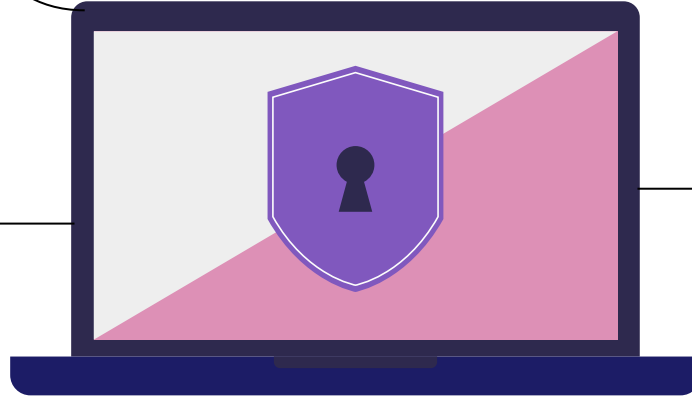
You need to decipher the secret message to move on to the next challenge !

Documents



Zip containing :

- secretmessage.txt
- readme.txt



HOW TO VALIDATE ?

Open the file of the CTF 3

CTF 2 - Resolution

```
kali@kali:~/Documents/CTF/crypto2$ cat secretmessage.txt
Kle qqbk ghdxpvrgh rmci iv ur kle vmqv dis rmci av flzw ckmpcinjq.
Wysw wti ymdgqr wmlhe eeh yrg azpl iuru mt.
Wti qmp smwjaoup mj xhh fcgi oi qrtvysfmfr uvqh wsr wtmj ghdxpvrgh.
```

```
kali@kali:~/Documents/CTF/crypto2$ cat readme.txt
Solve this challenge to access the next one. Should be easy when you find the key. It is right in front of your eyes ...
```

→ Vigenère cipher

CTF 2 - Resolution - Vigenère cipher

- Key and alphabet
- Add up the key to the clear text
- Can also use a table
- Powerful online tools (dcode.fr)

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

CTF 2 - Resolution

DÉCHIFFREMENT DE VIGENERE

★ MESSAGE CHIFFRÉ PAR VIGENERE

Kle qgbk ghdxpvrgh rmc i iv ur kle vmqv dis rmc i av flzw
ckmpcinjg.
Wysw wti ymdgqr wmlhe eeh yrg azpl iuru mt.
Wti gmp smwjaoup mj xhh fcgi oi qrtvysfmfr uvqh wsr wtmj
ghdxpvrgh.

PARAMÈTRES

★ LANGUE DU MESSAGE CLAIR Anglais (English) ▼

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

DÉCHIFFRER AUTOMATIQUEMENT

MÉTHODE DE DÉCHIFFREMENT

☒ AVEC LA CLÉ/LE MOT-CLÉ DE CHIFFREMENT: README

☐ AVEC LA LONGUEUR/TAILLE DE LA CLÉ, NOMBRE DE LETTRES : 6

☐ AVEC SEULEMENT UN MORCEAU DE LA CLÉ : CL?

☐ EN CONNAISSANT UN MOT DU TEXTE CLAIR : CODE

☐ CRYPTANALYSE DE VIGENERE (TEST DE KASISKI)

DÉCHIFFRER

Vigenere 🔑 README

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

The next challenge file is in the same zip file as this challenge.

Show the hidden files and you will find it.

The zip password is the type of encryption used for this challenge.

```
kali@kali:~/Documents/CTF/crypto2$ cat message.txt
The next challenge file is in the same zip file as this challenge.
Show the hidden files and you will find it.
The zip password is the type of encryption used for this challenge.
```

```
kali@kali:~/Documents/CTF/crypto2$ ls -a
.  ..  message.txt  .nextchallenge.zip  readme.txt  secretmessage.txt
```

Password of the zip = Vigenere

CTF 3 - Description

INSTRUCTIONS



You are given a basic pdf file and you need to find hidden information.

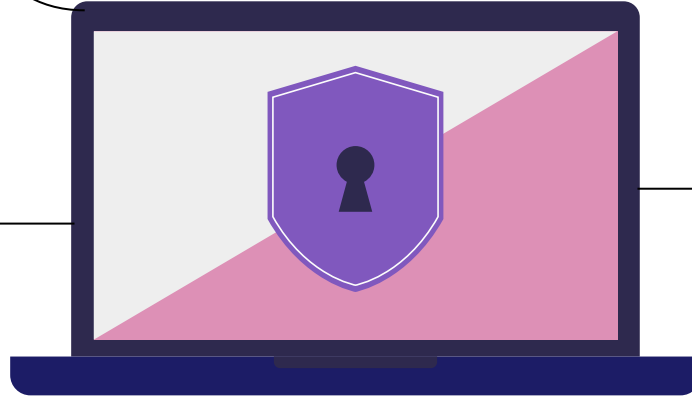
Documents



You need to solve CTF 2 to get these.

Zip containing :

- ElfCat.pdf
- readme.txt



HOW TO VALIDATE ?

Find the flag
(format "flag {...}")

CTF 3 - Resolution



Thank you for your attention

