# NeverLAN CTF

## **Reverse Engineering: Script Kiddie**

Value: 100 pts

Difficulty: Unknown

Description: It looks like a script kiddie was trying to build a crypto locker. See if

you can get the database back?

Attachment : encrypted db

### **Solution:**

Download the file «encrypted\_db» and open it.

6579776964584e6c636a45694f6e7369626d46745a534936496b746c5957
6468626942495a584a36623263694c434a3163325679626d46745a534936
496c4a7659326c7658307868596d466b0a61575531496977695a57316861
5777694f694a4b62334e6f64574666516d56705a58493051486c68614739
764c6d4e7662534973496d466b5a484a6c63334d694f6e7369633352795a
5756300a496a6f69516d396e61584e705932676754576c7a63326c766269
4973496e4e316158526c496a6f69515842304c6941344e4441694c434a6a
61585235496a6f69536d4635626d566962334a760a6457646f4969776965
6d6c775932396b5a534936496a63784e6a4d33496977695a325676496a70

It seem to be hexadecimal, all hash count number from 0 to 9 and letter from a to f. Let's decrypt all the hash from hexadecimal to text.

Source: <a href="http://www.unit-conversion.info/texttools/hexadecimal/">http://www.unit-conversion.info/texttools/hexadecimal/</a>

344d6a49694c434a6e5a5738694f6e736962474630496a6f694c544d314c 6a4d354e5451690a4c434a73626d63694f6949334e5334334e7a4577496e 31394c434a77614739755a534936496a41794e4330344e7a49744f54677a 4d7942344d546b354d6a59694c434a335a574a7a6158526c0a496a6f6959 6d4679636e6b75596d6c364969776959323974634746756553493665794a 755957316c496a6f6955324e6f626d56705a47567949433067536d466a62 324a7049697769593246300a5932685161484a68633255694f694a446458 4e3062323170656d4669624755676233423061573170656d6c755a794270 626e526c636d5a68593255694c434a6963794936496d5574596e567a0a61 57356c63334d6763336c756447686c63326c365a53427a5932686c625746 7a496e313966516f3d0a hex numbers to text eywidXNlcjEiOnsibmFtZSI6IktlYWdhbiBIZXJ6b2ciLCJ1c2VybmFtZSI6IlJvY21 vX0xhYmFk aWU1IiwiZW1haWwiOiJKb3NodWFfQmVpZXIOQH1haG9vLmNvbSIsImFkZHJ1c3MiOns ic3RvZWV0 IjoiQm9naXNpY2ggTW1zc21vbiIsInN1aXR1IjoiQXB0LiA4NDAiLCJjaXR5IjoiSmF 5bmVib3Jv dWdoIiwiemlwY29kZSI6IjcxNjM3IiwiZ2VvIjp7ImxhdCI6IjMzLjEyMjMiLCJsbmc NzM4In19LCJwaG9uZSI6IjAxNy0zOTctMTg4MSIsIndlYnNpdGUiOiJreXJhLmluZm8 iLCJjb21w YW55Ijp7Im5hbWUi0iJMYWJhZGl1LCBSZWluZ2VyIGFuZCBNY0dseW5uIiwiY2F0Y2h

#### The decoded output seem to be a base64, let's decode it too.

#### Source : <a href="https://www.base64decode.org/">https://www.base64decode.org/</a>

eywidXNlcjEiOnsibmFtZSI6IktlYWdhbiBIZXJ6b2ciLCJ1c2VybmFtZSI6IIJvY2lvX0xhYmFk aWU1liwiZW1haWwiOiJKb3NodWFfQmVpZXI0QHlhaG9vLmNvbSIsImFkZHJlc3MiOnsic3RyZWV0 IjoiQm9naXNpY2ggTWlzc2lvbilsInN1aXRIIjoiQXB0LiA4NDAiLCJjaXR5ljoiSmF5bmVib3Jv dWdoliwiemlwY29kZSI6ljcxNjM3liwiZ2Vvljp7lmxhdCl6ljMzLjEyMjMiLCJsbmciOil2NC4y NzM4In19LCJwaG9uZSI6IjAxNy0zOTctMTg4MSIsIndlYnNpdGUiOiJreXJhLmluZm8iLCJjb21w YW55Ijp7Im5hbWUiOiJMYWJhZGIILCBSZWiuZ2VyIGFuZCBNY0dseW5uliwiY2F0Y2hQaHJhc2UiOiJVc2VyLWNlbnRyaWMgZGVtYW5kLWRyaXZIbiBoYXJkd2FyZSIsImJzIjoiY29tcGVsbGluZyByZXB1cnBvc2UgaW5mcmFzdHJ1Y3R1cmVzIn19LCJ1c2VyMil6eyJuYW1lljoiQXNobGVpZ2ggT3NpbnNraSIsInVzZXJuYW1lljoiSG9ydGVuc2VfRWZmZXJ0ejE1liwiZW1haWwiOiJMaWxpYW5hLkZI ZW5leUBnbWFpbC5jb20iLCJhZGRyZXNzIjp7InN0cmVldCl6lktyYWpjaWsgR2F0ZXdheSIsInN1 aXRIIjoiU3VpdGUgMTQyIiwiY2l0eSI6lkNhcm9sY2hlc3RlciIsInppcGNvZGUiOiIzODk2My0w ODYyliwiZ2VvIjp7lmxhdCl6IjM3LjMxNDEiLCJsbmciOiltMTAyLjgwMjcifX0sInBob25lijoi KDIzMCkgMTI1LTU5MDMiLCJ3ZWJzaXRlIjoiZGV2aW4ubmV0liwiY29tcGFueSI6eyJuYW1lIjoi QW5rdW5kaW5nlC0gQ29sbGlucyIsImNhdGNoUGhyYXNlIjoiT3JnYW5pemVkIHJIZ2lvbmFslGNo For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page. ▼ Source character set. O Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set). < DECODE > Decodes your data into the textarea below. {"user1":{"name":"Keagan Herzog", "username":"Rocio\_Labadie5", "email":"Joshua\_Beier4@yahoo.com", "address": {"street":"Bogisich Mission", "suite":"Apt. 840", "city":"Jayneborough", "zipcode":"71637", "geo": {"lat":"33.1223", "lng":"64.2738"}}, "phone":"017-397-1881", "website":"kyra.info", "company":{"name":"Labadie, Reinger and McGlynn", "catchPhrase":"User-centric demand-driven hardware", "bs":"compelling repurpose infrastructures"}}, "user2": {"name":"Ashleigh Osinski", "username":"Hortense\_Effertz15", "email":"Liliana.Feeney@gmail.com", "address": {"street":"Krajcik Gateway", "suite":"Suite 142", "city":"Carolchester", "zipcode":"38963-0862", "geo":{"lat":"37.3141", "lng":"-102.8027"}}, "phone":"(230) 125-5903", "website":"devin.net", "company":{"name":"Ankunding - Collins", "catchPhrase":"Organized regional challenge", "bs":"frictionless whiteboard vortals"}}, "user3":{"name":"Iva D'Amore", "username":"Howell\_Pfannerstill", "email":"Jarred\_Deckow@gmail.com", "address":{"street":"Olson Glens", "suite":"Apt. 870", "city":"South Donaldburgh", "zipcode":"07601-7976", "geo":{"lat":"36.9448", "lng":"-96.7118"}}, "phone":"454.213.5840 x5846", "website":"petra.com", "company":{"name":"Gulgowski Inc", "catchPhrase":"Reactive bi-directional process improvement", "bs":"cross-platform orchestrate niches"}}, "user4": "name":"Augustine Kreiger", "username":"Kamron\_Williamson89", "email":"Trever\_Hickle@gmail.com", "address": {"street":"075022", "geo":{"lat":"-77.4075", "lng":"-"street":"Alisa View","suite":"Apt. 797","city":"Rosalynbury","zipcode":"95522","geo":{"lat":"-77.4075","Ing":

Save the output into a file (i called it decrypted\_db). Open it with leafpad or something and use the function «Search» for search the «flag» keyword.

"flag{ENC0D1NG\_D4TA\_1S\_N0T\_ENCRY7I0N}",

Flag: flag{ENC0D1NG\_D4TA\_1S\_N0T\_ENCRY7I0N}