



SERVICIUL DE
TELECOMUNICAȚII
SPECIALE

Introducere în

CTF - CAPTURE THE FLAG

www.sts.ro

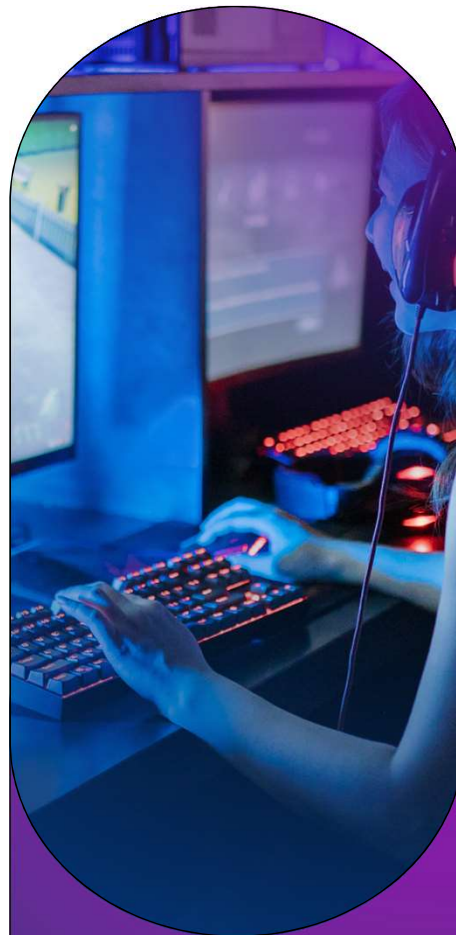
IULIE 2025

Ce sunt CTF-urile?

Competițiile de tip **CTF (Capture The Flag)** sunt concursuri de securitate cibernetică care oferă o oportunitate excelentă de a vă testa și de a vă îmbunătăți abilitățile de securitate și de rezolvare a problemelor.

Prin provocări de hacking cu diferite niveluri de dificultate și moduri de rezolvare, aceste concursuri evaluează abilitățile și cunoștințele despre securitatea cibernetică, munca în echipă și creativitatea.

Participarea poate fi individuală sau în echipă, iar punctajul depinde de dificultatea provocării și timpul de rezolvare.





Tipuri de competiții CTF

Jeopardy

- Cel mai de **întâlnit** tip de CTF
- Fiecare provocare necesită găsirea unui **"flag"** pentru care se acordă **puncte**
- Multiple categorii de provocări: web, crypto, pwn, reverse, steganografie, etc.

King of the Hill

- Scopul este să **preiei controlul** asupra unui sistem (Ex. o mașină virtuală) și să **rămâi în posesia** lui cât mai mult timp
- Echipele se luptă simultan pentru acces, modificând parole, configurând backdoor-uri sau ștergând accesul altora
- Accentul e pus pe menținerea **persistenței** și **strategie** în timp real

Attack & Defense

- Echipele primesc același sistem vulnerabil
- Trebuie să-l **apere** și, în același timp, să **atace** sistemele celorlalți.
- Necesită experiență în rețelistică, administrare de servere și dezvoltare de exploit-uri

Hybrid

- Combină mai multe tipuri, spre exemplu Jeopardy + Attack-Defense
- Se întâlnește la finalele unor competiții importante
- Mai greu de organizat, dar extrem de provocator

Ce tipuri de provocări există?

Web

Exploatarea vulnerabilităților din aplicații web: SQLi, XSS, command injection

Crypto

Implică spargerea mesajelor criptate sau exploatarea unor algoritmi de criptare slabi sau implementați necorespunzător

Forensics

Analiza fișierelor PCAP, imagini de disc, dump-uri de memorie sau jurnalizări pentru a descoperi informații ascunse sau dovezi digitale

Steganografie

Ascunderea de date în imagini, fișiere video sau audio

Reverse engineering

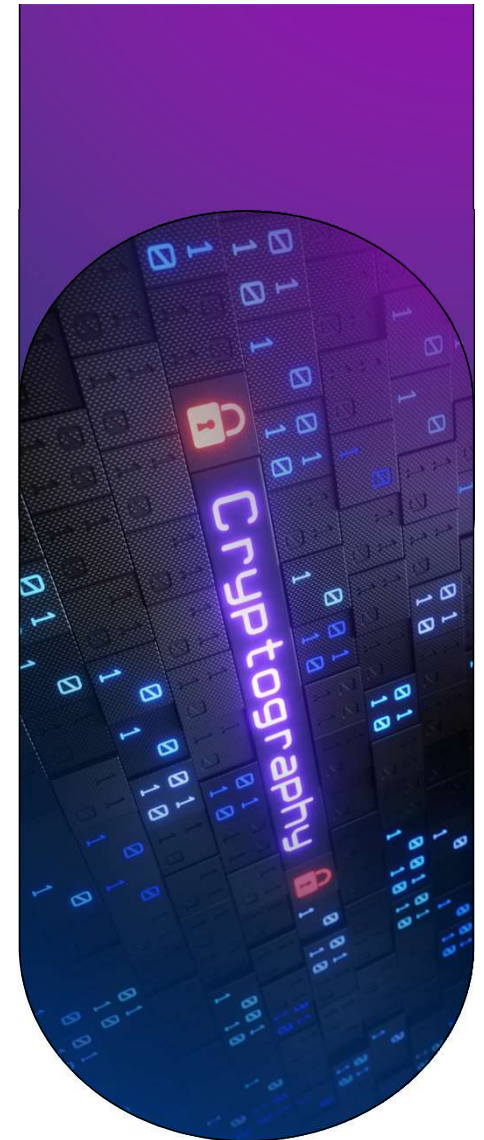
Analiza codului executabil pentru a înțelege cum funcționează

Binary Exploitation/Pwn

Găsirea și exploatarea vulnerabilităților din fișiere executabile

Misc

Provocări diverse, uneori de logică sau cultură generală





Cine poate participa?

Începători / Studenți

- Ideal pentru studenți la informatică, automatică, matematică sau inginerie
- Multe CTF-uri sunt educaționale, axate pe învățare prin practică
- Platforme ca picoCTF sau TryHackMe sunt concepute special pentru începători

Profesioniști / Specialiști IT

- Este o oportunitate de perfecționare în domenii precum pentesting, sysadmin, devsecops, analiză malware
- Participă pentru a-și menține abilitățile actualizate sau pentru a experimenta tehnici noi într-un mediu controlat

Unde se desfășoară?

Majoritatea CTF-urilor sunt online, deci poți participa de oriunde, iar unele competiții din cadrul unor conferințe mari precum DEFCON, DEFCAMP, prezența este fizică.

Ce ai nevoie ca să participi?

- Trei aspecte sunt importante ca să poți participa la un CTF: **curiozitatea, perseverența și dorința de a învăța**
- Oricine poate începe — fie că ești elev, student sau profesionist în domeniul IT
- Cunoștințele de bază în Linux, programare, rețelistică sau criptografie sunt utile, dar nu obligatorii. De cele mai multe ori, înveți pe parcurs, direct din provocări

Ce tool-uri sunt folosite?

Generale

- Kali Linux, Parrot OS – sisteme de operare cu multe tool-uri preinstalate
- Google & Writeups – căutarea este o unealtă esențială
- Notepad++, VS Code – analiză și editare fișiere

Web

- Burp Suite, Postman – testare și manipulare de cereri HTTP
- SQLmap – detecție și exploatare SQL injection

Crypto

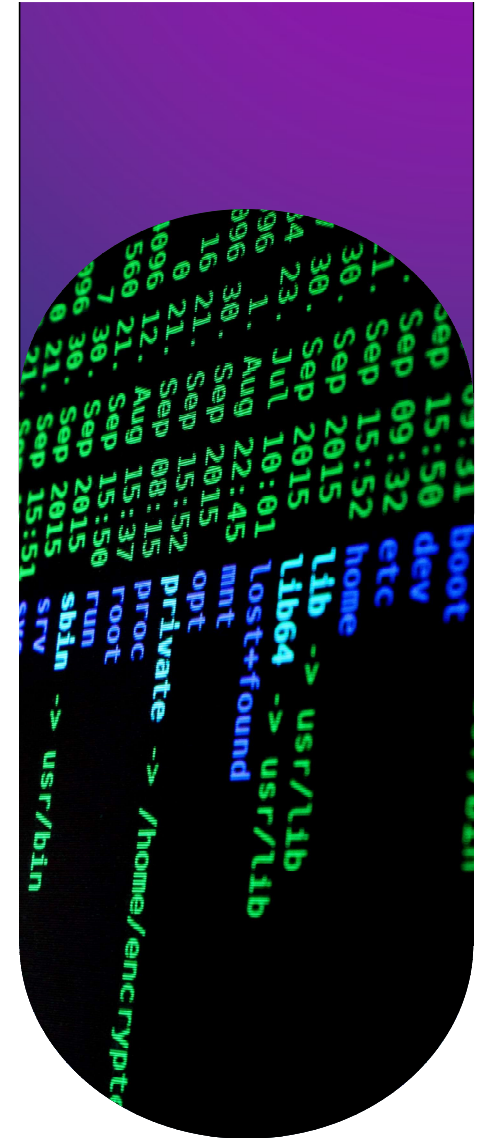
- CyberChef – decodare, criptare, transformări rapide
- SageMath – calcule matematice avansate

Forensics

- Wireshark – analiză trafic de rețea (PCAP-uri)
- binwalk – extragere de date din fișiere binare
- Volatility – analiză de memorie RAM
- comenzi: file, strings, foremost, exiftool – analiză fișiere suspecte

Pwn / Binary Exploitation

- Ghidra, IDA Free – reverse engineering
- GDB, pwndbg, pwntools – debugging și exploit scripting



Cum arată o provocare?

Categorie: Crypto – Cifrul Cezar

Provocare:

Am interceptat un mesaj criptat. Se pare că a fost folosit un cifru Cezar.
Poți să găsești flag-ul?

fliuxo fhcdv hvwh lqwhuhvdqw!

Ce faci?

- Știi că un cifru Cezar deplasează literele alfabetului.
- Încerci să inversezi criptarea cu o shiftare de 3 (cea mai comună valoare).
- Mesajul devine:

cifrul cezari este interesant!

În funcție de format, flag-ul poate fi:

flag{cifrul cezari este interesant!}

Flag: cifrul cezari este interesant!



Rezolvare în CyberChef

În CyberChef cifrul
Cezar poate fi spart cu
ajutorul operației
ROT13 modificată

The screenshot displays the CyberChef interface with the following components:

- Operations List:** A sidebar on the left containing various operations. The 'rot' operation is selected, and the 'ROT13' option is highlighted. An arrow points from the red text annotation to this selection.
- Recipe Panel:** The central panel shows the 'ROT13' recipe configuration. It includes checkboxes for 'Rotate lower case chars' (checked), 'Rotate upper case chars' (checked), and 'Rotate numbers' (unchecked). Below these, the 'Amount' is set to '-3'. An arrow points from the red text annotation to this field.
- Input Field:** The top right section contains the input text: 'fliuxo fhcdv hvwh lqwhuhvdqw!'. An arrow points from the red text annotation to this field.
- Output Field:** The bottom right section shows the decrypted output: 'cifrul cezar este interesant!'. An arrow points from the red text annotation to this field.
- Buttons:** At the bottom of the recipe panel, there are buttons for 'STEP', 'BAKE!' (highlighted in green), and 'Auto Bake' (checked).

Red text annotations with arrows provide instructions: 'Se adaugă textul cifrat prezent în provocare' points to the input, 'Se modifică valoarea rotației care se va face pentru fiecare literă' points to the amount field, and 'Se obține textul decriptat' points to the output.

Bootcamp STS

Participanți: 20 de studenți

Loc de desfășurare: București și Brașov

Durata: 7 zile

**Subiecte abordate prin activități hands-on
și lucru în echipă:**

- comunicații securizate voce-video-date
- rețelistică
- dezvoltare software
- cloud computing
- cybersecurity
- blockchain
- infosec
- infrastructuri critice



www.bootcamp.sts.ro







**SERVICIUL DE
TELECOMUNICAȚII
SPECIALE**

CHALLENGE-URI

www.sts.ro

IULIE 2025

#1

Look

Categorie: Steganografie

Descriere:

Încearcă să găsești flag-ul ascuns în imagine. Este o provocare simplă de steganografie – mesajul este ascuns într-un mod subtil în fișierul imagine.

Task:

Poți să citești în binar?

Timp rezolvare: 5 min

Link descărcare:

<https://files.stscloud.ro/s/b9ysXgrnrRotjHQ>

Parola:

Parola_look1





SOLUȚIE

Look

Imaginea conține o secvență de caractere formate din 0 și 1, care pare a fi un text scris în binar. Pentru a putea decodifica mesajul, trebuie mai întâi să extragem conținutul binar din imagine.

În loc să copiem manual fiecare cifră, putem folosi un instrument de tip OCR (Optical Character Recognition), care recunoaște automat textul din imagine. Un exemplu simplu este <https://www.onlineocr.net>, care transformă imaginea într-un text editabil.

După extragerea textului, acesta poate fi convertit din binar în ASCII pentru a obține flag-ul.

#1

SOLUȚIE

onlineocr.net

OCR HOMEOCR APIBONUS PROGRAMPDF TO WORDPDF TO EXCELPDF TO DOCPDF TO IMAGE

IMAGE TO TEXT CONVERTER - OCR ONLINE

Picture to text converter allows you to extract text from image or convert PDF to Word, Excel or Text formats using Optical Character Recognition software online

Advertisement

1 STEP - Upload image

2 STEP - Select language and output format

3 STEP - Convert image

SELECT FILE...

ENGLISHMicrosoft Word (.docx)

CONVERT

look.png

Download Output File

01000110 01101100 01100001 01100111 00111010 00100000 01100010 01100010 00110000 00110111 01100101 01100110 00110000 00110011 00110001 00110110 00110010 00110001 00110001 00110000 01100011 00110011 01100011 0110010 00110000 00110011 00110010 00110010 01100010 00110101 00111000 00111000 01100100 01100001 00111001 00110011 01100101

Acum putem copia textul binar si să îl introducem în orice tool online care poate transforma din binar în ASCII, spre exemplu CyberChef.

#1

SOLUȚIE

The screenshot shows a web-based tool interface with three main sections: **Operations**, **Recipe**, and **Input/Output**.

- Operations:** A list of operations including "To Binary", "From Binary", "AMF Decode", "AMF Encode", "BSON deserialise", "BSON serialise", "CBOR Decode", "CBOR Encode", "From BCD", and "From MessagePack".
- Recipe:** A configuration area for the "From Binary" operation. It includes a "Delimiter" set to "Space" and a "Byte Length" set to "8". At the bottom, there is a "BAKE!" button and an "Auto Bake" checkbox.
- Input:** A text area containing a long string of binary data (0s and 1s).
- Output:** A text area displaying the result: "Flag: bb07ef031662110c3c20322b588da93e".

- Textul în binar se copiază în câmpul **Input**.
- În **Operations** se caută funcția **From Binary**. Drag and drop în câmpul **Recipe**.
- În câmpul **Output** va apărea flag-ul căutat.

Flag: bb07ef031662110c3c20322b588da93e

#2

SOLUȚIE

There is more

Categorie: Steganografie

Descriere:

Încearcă să găsești flag-ul ascuns în imagine. Extrageți datele necesare și veți obține ceea ce căutați.

Task:

Poți extrage metadatele și să găsești flag-ul?

Timp rezolvare: 5 min

Link descărcare:

<https://files.stscloud.ro/s/knkNnJ3Zpe3R8Dc>

Parola:

Parola_more1



#2

SOLUȚIE

There is more

Numele provocării, descrierea și chiar conținutul imaginii (unde cuvântul „metadata” este evidențiat) sugerează clar că atenția trebuie îndreptată către metadatele fișierului, nu către imaginea în sine.

Metadatele unei poze sunt informații ascunse în fișierul imaginii, cum ar fi data realizării, modelul camerei, locația GPS sau comentarii adăugate. Acestea nu sunt vizibile direct, dar pot fi extrase cu unelte speciale precum **exiftool**, un instrument foarte util disponibil în Kali Linux.

Pași:

- Ne mutăm în terminal în directorul unde se află imaginea.
- Rulăm comanda:
 - **exiftool there_is_more.png**
- Verificăm informațiile afișate și se observă că flag-ul căutat este în câmpul **Image Description**

#2

SOLUȚIE

```
(kali㉿kali)-[~/Desktop/CTF]
└─$ ll
total 372
-r-r-xr-x 1 kali kali 380499 Sep 20 2022 there_is_more.png

(kali㉿kali)-[~/Desktop/CTF]
└─$ exiftool there_is_more.png
ExifTool Version Number      : 13.00
File Name                    : there_is_more.png
Directory                    : .
File Size                     : 380 kB
File Modification Date/Time   : 2022:09:20 10:08:56-04:00
File Access Date/Time        : 2025:06:16 03:20:17-04:00
File Inode Change Date/Time   : 2025:06:16 03:20:17-04:00
File Permissions              : -r-xr-xr-x
File Type                    : PNG
File Type Extension          : png
MIME Type                    : image/png
Image Width                   : 895
Image Height                  : 505
Bit Depth                     : 8
Color Type                    : RGB with Alpha
Compression                   : Deflate/Inflate
Filter                        : Adaptive
Interlace                     : Noninterlaced
Warning                       : [minor] Text/EXIF chunk(s) found after PNG IDAT (may be
ignored by some readers)
Exif Byte Order               : Big-endian (Motorola, MM)
Image Description             : Flag: 15D6DE33A771B23E928FEA242ACC1F75
Resolution Unit               : inches
Y Cb Cr Positioning           : Centered
Image Size                    : 895x505
Megapixels                    : 0.452

(kali㉿kali)-[~/Desktop/CTF]
└─$
```

Flag: 15D6DE33A771B23E928FEA242ACC1F75

#3

Text matters

Categorie: Steganografie

Descriere:

Încearcă să găsești flag-ul ascuns în imagine. Țineți cont de toate informațiile și veți obține ceea ce căutați.

Task:

Un tool cunoscut a fost folosit pentru a ascunde un mesaj. Crezi că îl poți găsi?

Timp rezolvare: 5 min

Link descărcare:

<https://files.stscloud.ro/s/wX89tHTooKoRJrA>

Parola:

Parola_text1



#3

SOLUȚIE

Text matters

Imaginea conține textul "Keep looking...", iar descrierea sugerează că, folosind un tool cunoscut, un mesaj a fost ascuns în fișierul imagine. Indiciul din titlu lasă de înțeles că textul are o importanță aparte – „textul contează”.

Steghide este un instrument popular și puternic folosit pentru a ascunde date (texte, fișiere) în fișiere multimedia, în special în imagini și fișiere audio. Acesta ascunde informația în mod discret, modificând cel mai puțin vizibil bitii fișierului gazdă, astfel încât modificările să fie aproape imposibil de detectat cu ochiul liber.

Indiciul ne sugerează că asupra imaginii s-a folosit steghide, așa că putem încerca să extragem datele ascunse cu același tool.

Numele fișierului, „text_matters”, ne dă de înțeles că textul din imagine este important și, foarte probabil, parola pentru extragere este chiar textul vizibil („Keep looking...”).

Tot ce rămâne este să testăm această parolă folosind comanda steghide extract până reușim să scoatem conținutul ascuns cu succes.

#3

SOLUȚIE

```
(kali㉿kali)-[~/Desktop/CTF]
$ steghide extract -sf text_matters.jpg -p Keeplooking...
wrote extracted data to "secret.txt".

(kali㉿kali)-[~/Desktop/CTF]
$ cat secret.txt
Flag: 9435ABC2ACF24086C3128DE6B71B2DE0
```

Flag: 9435ABC2ACF24086C3128DE687182DE0

#4

2 IN 1

Categorie: Crypto

Descriere:

Flag-ul este în fișierul 2in1.txt, încearcă să îi obții.

Task:

Reușești să decodifici mesajul ascuns prin mai multe niveluri de codificare?

Timp rezolvare: 5 min

Link descărcare:

<https://files.stscloud.ro/s/SQTQ8rLzPqKj8aC>

Parola:

Parola_2_in_1



#4

SOLUȚIE

2 IN 1

Textul conține grupuri de câte două caractere (ex: 52, 6d, 78), fiecare fiind un număr hexazecimal (0-9, a-f). Aceasta indică faptul că datele sunt codificate în format hexazecimal.

Hexazecimalele nu sunt de obicei separate prin „+”, ci prin spațiu, fără spațiu sau cu prefixul „\x”. Așadar, primul pas este să înlocuim toate semnele „+” cu spațiu, pentru a obține un șir continuu de hexazecimale.

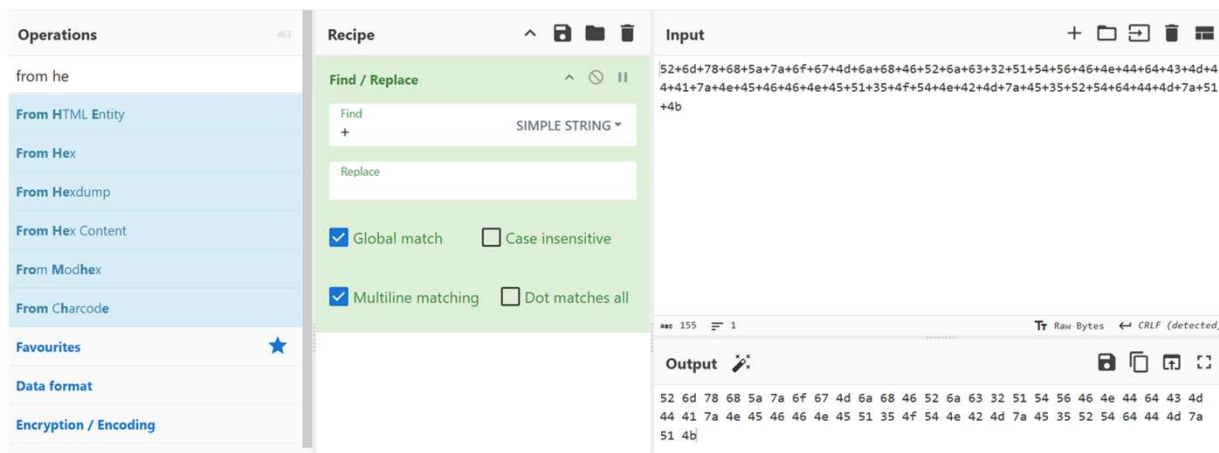
Folosind CyberChef sau un alt tool, aplicăm operația From Hex pentru a converti șirul hexazecimal într-un text ASCII.

După decodare, obținem un șir ce pare a fi în format Base64.

Aplicăm operația From Base64 în CyberChef pentru a obține textul clar.

#4

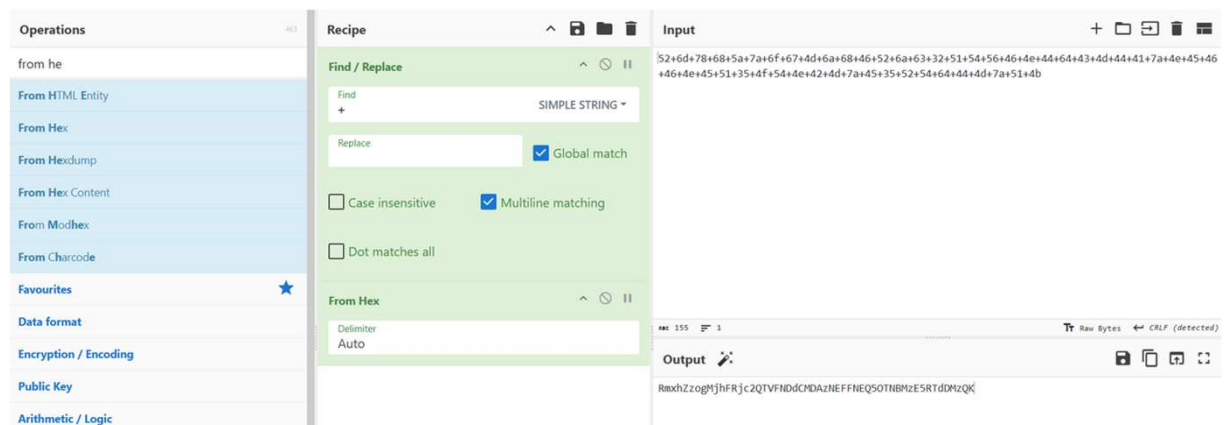
SOLUȚIE



Folosim funcția **Find / Replace** din CyberChef pentru a înlocui toate semnele „+” cu spațiu.

#4

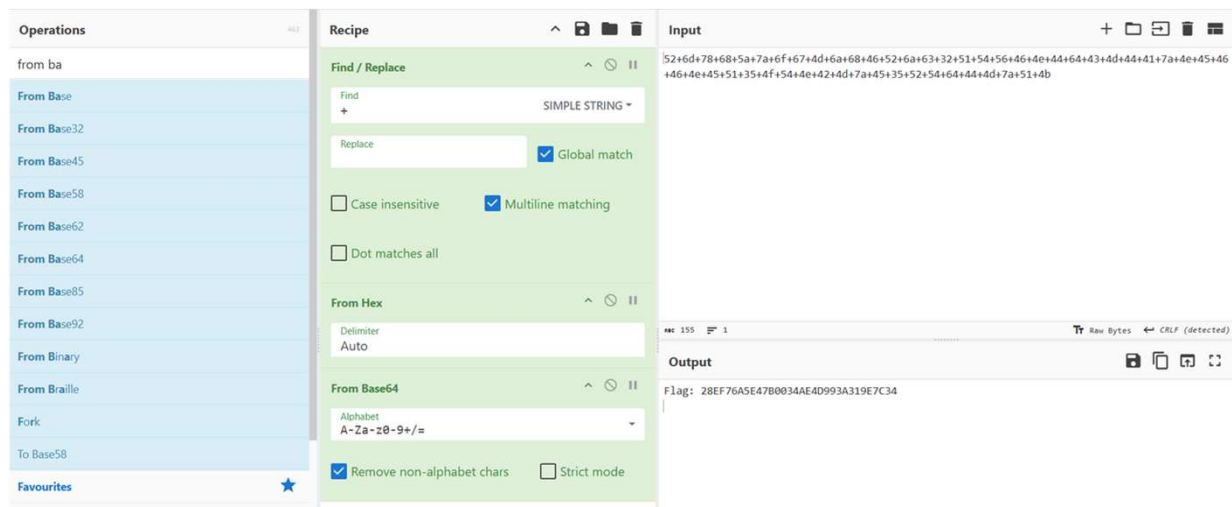
SOLUȚIE



Următorul pas este să aplicăm funcția **From Hex** peste output-ul obținut anterior și va rezulta un string encodat in Base64.

#4

SOLUȚIE



Aplicând și funcția **From Base64** peste output-ul obținut anterior va rezulta flag-ul căutat.

Flag: 28EF76A5E47B0034AE4D993A319E7C34

#5

Spacedot

Categorie: Crypto

Descriere:

Fișierul spacedot.txt conține o secvență formată doar din spații și puncte.
Încearcă să obții flag-ul.

Task:

Observi unde este ascuns flag-ul?

Timp rezolvare: 5 min

Link descărcare:

<https://files.stscloud.ro/s/kbx3YwaT6faAoa3>

Parola:

Parola_spacedot1



#5

SOLUȚIE

Spacedot

Putem observa că fișierul conține doar două simboluri: spațiu și punct, ceea ce sugerează o codificare binară ascunsă. Chiar dacă o căutare pe internet pentru "space dot encoding" nu oferă rezultate utile, putem deduce că:

- punctul (.) poate fi considerat ca 1
- spațiul () poate fi considerat ca 0

Pentru a face conversia, putem folosi tool-ul CyberChef:

- Căutăm funcția **Replace** în coloana din stânga.
- O aplicăm de două ori:
 - Prima dată: (.) → 1
 - A doua oară: () → 0
- Atenție - selectați tipul **"Simple String"** și nu **"Regex"**, deoarece punctul (.) este caracter special în expresiile regulate și înlocuirea poate eșua.

După înlocuire, folosim funcția **From Binary** pentru a transforma șirul de biți în text **ASCII**, unde flag-ul devine vizibil.

SOLUȚIE



#5

SOLUȚIE

The screenshot displays a binary manipulation tool interface with three main panels:

- Operations:** A list of operations on the left, including "To Binary", "From Binary", "AMF Decode", "AMF Encode", "BSON deserialise", "BSON serialise", "CBOR Decode", "CBOR Encode", "From BCD", "From MessagePack", "To BCD", "To MessagePack", and "YARA Rules".
- Recipe:** A central panel showing a sequence of operations:
 - Find / Replace:** Find: *, Replace: 1. Options: ☒ Global match, ☐ Case insensitive, ☒ Multiline matching, ☐ Dot matches all.
 - Find / Replace:** Find: *, Replace: 0. Options: ☒ Global match, ☐ Case insensitive, ☒ Multiline matching, ☐ Dot matches all.
 - From Binary:** Delimiter: Space, Byte Length: 8.
- Input:** A text area containing a long string of asterisks representing binary data.
- Output:** A text area showing the result: "Hello! Flag: 5BCE77980D58261EF03F47BFCCB4A67E".

Flag: 5BCE77980D58261EF03F47BFCCB4A67E

#6

Correct String

Categorie: Reverse

Descriere:

Flag-ul este ascuns în codul din fișier, dar este plin și cu multiple flag-uri incorecte. Provocarea este să identifici și să extragi flag-ul real dintre toate informațiile false folosind indiciile prezente.

Task:

Care este flag-ul corect?

Timp rezolvare: 10 min

Link descărcare:

<https://files.stscloud.ro/s/H8oqNr2LEXqkmgd>

Parola:

Parola_corect1



#6

SOLUȚIE

Correct String

Din titlul challenge-ului, „**Correct String**”, deducem că flag-ul poate fi găsit folosind comanda **strings**, care extrage toate șirurile de caractere lizibile dintr-un fișier binar. Astfel, putem scăpa rapid de datele binare și de falsurile care nu sunt stringuri clare și să căutăm flag-ul real printre rezultatele afișate.

La o primă vedere, prezența șirului „**UPX!**” în output-ul comenzii strings indică faptul că executabilul este împachetat cu **UPX**. Aceasta împiedică accesul direct la codul real și, implicit, la flag.

Packerele sunt programe sau utilitare care comprimă sau criptează un fișier executabil pentru a-i reduce dimensiunea sau pentru a-i ascunde conținutul real. În contextul securității cibernetice, packerele sunt folosite adesea pentru a împiedica analiza codului de către tool-uri automate de securitate precum Antivirushi sau Firewall, mascând structura internă a programului.

Pentru a putea analiza fișierul și a căuta flag-ul, trebuie mai întâi să despachetăm executabilul folosind comanda: **upx -d <nume_executabil>**

După despachetare, putem folosi din nou comanda strings pentru a extrage toate șirurile lizibile și a identifica flag-ul corect.

#6

SOLUȚIE

```
(root@DESKTOP-DDVAOUP)-[/home/kali]
# strings correctString | more
4UPX!4
iYa/
/PB_
8/h]
X/0GP
H/ '
WAPRH
D24!
)ARVAUATUS
[]A\A
```

```
(root@DESKTOP-DDVAOUP)-[/home/kali]
# strings correctString | grep UPX
4UPX!4
$Info: This file is packed with the UPX executable packer http://upx.sf.net $
$Id: UPX 3.94 Copyright (C) 1996-2017 the UPX Team. All Rights Reserved. $
UPX!u
UPX!
UPX!
```

Se observă faptul că fișierul a fost obfuscat folosind packer-ul **UPX**, astfel că vom folosi utilitarul **upx** prezent în **Kali Linux** pentru a obține codul sursă real.

#6

SOLUȚIE

```
(root@DESKTOP-DDVAOUP)-[/home/kali]
# upx -d correctString
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2024
UPX 4.2.2      Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 3rd 2024

  File size      Ratio      Format      Name
-----
  846090 <-    332408    39.29%    linux/amd64  correctString

Unpacked 1 file.
```

Folosind comanda **upx -d correctString** a fost despachetat codul sursă, iar folosind din nou comanda **strings** putem observa că acesta pare să fie în forma corectă și inteligibilă.

```
(root@DESKTOP-DDVAOUP)-[/home/kali]
# strings correctString | more
5,.
WAPRH
AWAVAUATUSH
[]A\A]A^A_
u'UH
Flag: isI
not herL
PasswordH
is 1234H
567890!
Packers H
gona pach
```

#6

SOLUȚIE

Cautăm cuvântul cheie **Flag** în tot fișierul și observăm că apare în mai multe locuri, deci este posibil ca flag-ul să se afle pe următoarele linii.

```
(kali@kali)-[~/Desktop/CTF]
$ strings correctString -n 8 | grep -i flag
Flag: isI
Flag: miH
s[Flag iH
WARNING: Unsupported flag value(s) of 0x%x in DT_FLAGS_1.
s->_Flags2 & _IO_FLAGS2_FORTIFY
version = NULL || (Flags & ~(DL_LOOKUP_ADD_DEPENDENCY | DL_LOOKUP_GSCOPE_LOCK)) = 0
imap->l_type = lt_loaded && (imap->l_flags_1 & DF_1_NODELETE) = 0
_dl_x86_hwcaps_flags
_dl_stack_flags
```

Se modifică comanda de mai sus, adăugând opțiunea **-A 10** pentru comanda **grep**, pentru a afișa și următoarele 10 rânduri după fiecare apariție a cuvântului cheie **Flag**.

```
(kali@kali)-[~/Desktop/CTF]
$ strings correctString -n 8 | grep -i flag -A 10
Flag: isI
not herL
PasswordH
is 1234H
Packers H
gona pach
01010101H
11110101H
01010010H
10000000H
00111100H
--
Flag: miH
char pasH
s[Flag iH
466c6167H
3a203039H
43384538H
37443131H
33303945H
37323631H
37383133H
30383038H
38314545
SysfaultH
--
WARNING: Unsupported flag value(s) of 0x%x in DT_FLAGS_1.
setup_vdso
elf_get_dynamic_info
AVX512CD
AVX512BW
AVX512DQ
AVX512ER
AVX512PF
AVX512VL
Slow_BSF
AVX_Usable
--
s->_Flags2 & _IO_FLAGS2_FORTIFY
** invalid %N$ use detected **
(unsigned int) done < (unsigned int) INT_MAX
(size_t) done < (size_t) INT_MAX
** %n in writable segment detected **
printf_positional
```

#6

SOLUȚIE

Încercăm să decodăm toate șirurile obținute. Din primul nu se obține nimic relevant.

Operations: 463

binar

To Binary

From Binary

AMF Decode

AMF Encode

BSON deserialise

BSON serialise

CBOR Decode

Recipe

From Binary

Delimiter: Space

Byte Length: 8

Input

01010101
11110101
01010010
10000000

Raw Bytes CRLF (detected)

Output

l0R

Dar folosind al doilea șir identificat se obține flag-ul căutat.

Operations: 463

hex

To Hex

From Hex

Hex to PEM

PEM to Hex

To Hexdump

From Hexdump

To Hex Content

Recipe

From Hex

Delimiter: Auto

Input

466c6167
3a203039
43384538
37443131
33303945
37323631
37383133
30383038
3831

Raw Bytes CRLF (detected)

Output

Flag: 09C8E87D11309E72617813080881



**SERVICIUL DE
TELECOMUNICAȚII
SPECIALE**

MULȚUMESC

www.sts.ro

IULIE 2025