



Ghid pentru profesori, antrenori și participanți

Introducere în UNbreakable România, ediția 2026

unbreakable.ro

Introducere	4
Ce înseamnă securitatea cibernetică și de ce este un subiect important?	4
Ce este UNbreakable România?	6
Despre concurs	6
Rezultate UNbreakable România 2020-2025	6
Către UNbreakable România 2026	7
Cui se adresează?	8
De ce să participi la UNbreakable România?	9
Care este programul UNbreakable România și ce se întâmplă în fiecare etapă?	11
Competiții locale de pregătire	11
Etapă de pregătire și antrenament	11
Concursul pe echipe - online	11
Concursul pe echipe - fizic (finala UNbreakable România)	12
Misiunea UNbreakable România	12
Pregătirea participanților pentru UNbreakable România	12
Care sunt regulile și limitările generale pentru participanți?	12
Care sunt și cum se calculează criteriile de evaluare?	13
Nivelul de dificultate al exercițiilor	13
Scorul pe etapă	13
Punctajul unui exercițiu - exerciții de tip Jeopardy	14
Scorul pe sezon	14
Ce înseamnă clasamentul pe județ, liceu sau universitate - #ROEduCyberSkills	15
Care sunt grupele în care poate fi încadrat un participant?	16
Cum se poate pregăti un participant pentru UNbreakable România?	16
Care sunt oportunitățile de dezvoltare în afară de UNbreakable România pentru elevi și studenți?	17
Care sunt resursele necesare pentru a putea participa la competiții?	18
Cum pot adresa întrebări Organizatorilor sau Mentorilor?	18
Pregătire antrenori și profesori pentru UNbreakable România	19
Care este rolul unui antrenor sau profesor?	19
Cum mă pot înscrie ca antrenor sau profesor pentru a reprezenta o instituție de învățământ?	19
Cum pot urmări activitatea participanților?	20
Cum se vor alcătui echipele?	20
Cum vor fi selecționați finaliștii pentru faza finală?	20
Exemple de exerciții	20
Care sunt tipurile de exerciții?	20
Tipuri de exerciții	20
Nivelul de dificultate al exercițiilor	20
Cum arata un flag / steag?	21
Cum pot obține un flag / steag?	21

Cum arată un exercițiu teoretic?	21
Exemplu exercițiu teoretic #1	21
Exemplu exercițiu teoretic #2	22
Cum arată un exercițiu practic?	22
Exemplu exercițiu practic #1	22
Exemplu exercițiu practic #2	23
Ce sistem de operare ar trebui folosit în timpul concursului?	24
Implicare și suport	25
Cum pot deveni mentor?	25
Ce înseamnă mentorat?	25
Ce rol au mentorii?	25
Responsabilitatea unui mentor	25
Cum poate instituția noastră să devină partener al evenimentului?	25
Care sunt principalele beneficii de participare pentru un liceu sau o universitate?	25
Cum se poate implica un liceu sau o universitate?	26
Cum pot fi susținuți studenții?	26
Ce resurse sunt disponibile pentru a-i pregăti pe studenți?	26
Cum pot contribui la dezvoltarea resurselor pentru participanți?	27
Cum poți contacta organizatorii?	27

Introducere

Ce înseamnă securitatea cibernetică și de ce este un subiect important?

Securitatea cibernetică este o ramură a informaticii care se ocupă cu identificarea riscurilor implicate de folosirea dispozitivelor inteligente precum calculatoare, smartphone-uri, dar și rețele de calculatoare, atât publice cât și private, și cu oferirea de soluții pentru înlăturarea lor. Este o componentă vitală pentru organizații, dar și pentru oameni.

Atacurile cibernetice și criminalitatea informatică sunt tot mai numeroase și mai sofisticate în toată Europa. Se preconizează că această tendință va continua să crească în viitor, date fiind previziunile conform cărora aproape 30 de miliarde de dispozitive la nivel mondial vor fi conectate la internetul obiectelor (Internet of Things) până în 2030.

Securitatea cibernetică trebuie să țină pasul cu evoluția rapidă a tehnologiilor emergente, precum Inteligența Artificială (AI), care aduce atât oportunități, cât și provocări. AI a fost deja integrată în procesele de afaceri, optimizând fluxurile de lucru și reducând necesarul de expertiză în unele cazuri. AI influențează și securitatea cibernetică, fiind utilizată pentru generarea de deepfakes și pentru crearea de mesaje de phishing mai convingătoare. Modelele lingvistice mari (LLMs) sunt folosite și de hackeri pentru identificarea rapidă a vulnerabilităților și crearea de exploatări mai sofisticate, ceea ce face ca protecția sistemelor să devină din ce în ce mai dificilă. Astfel, este esențial ca organizațiile să adopte soluții de securitate proactive, care să răspundă acestei noi realități tehnologice.

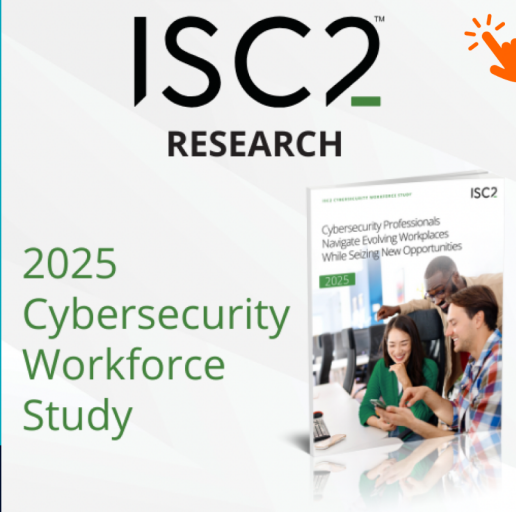
De asemenea, în ultimele luni, s-a observat o tendință îngrijorătoare pe platformele de socializare, unde pagini cu un număr semnificativ de urmăritori utilizează imagini generate de AI, extrem de realiste. Aceste imagini sunt adesea percepute ca autentice de către utilizatori, care, din lipsa unui fundament tehnic solid, devin vulnerabili la dezinformare. Această situație reflectă o lacună în educația digitală, mai ales în contextul avansului rapid al tehnologiilor emergente. În paralel, unele platforme de social media continuă să faciliteze răspândirea de informații false, iar veridicitatea acestora devine tot mai dificil de evaluat, ceea ce crește riscurile de manipulare a opiniei publice. Aceste fenomene subliniază necesitatea implementării unor soluții avansate de securitate cibernetică și educație digitală, pentru a contracara riscurile asociate cu utilizarea AI în scopuri malițioase și pentru a proteja utilizatorii de amenințările emergente.

UE își consolidează capacitatea de a proteja Europa de amenințări cibernetice și de a stimula competitivitatea sectorului securității cibernetice din UE. Negociatorii Consiliului și ai Parlamentului European au ajuns la un acord cu privire la o propunere de înființare a unui Centru de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a unei rețele de centre naționale de coordonare. Împreună, aceste structuri vor contribui la securizarea pieței unice digitale,

inclusiv în domenii precum comerțul electronic, mobilitatea inteligentă și internetul obiectelor, și la sporirea autonomiei UE în domeniul securității cibernetice.

Noul centru de competențe, cu sediul la București, împreună cu rețeaua de centre naționale de coordonare desemnate de statele membre, va ajuta UE să pună în comun și să transmită în rețea cunoștințele sale de specialitate în domeniul cercetării, tehnologiei și dezvoltării industriale în materie de securitate cibernetică și să promoveze implementarea celor mai recente soluții de securitate cibernetică.

Pe măsură ce organizațiile își extind amprenta digitală, devine imperativ să fie protejate disponibilitatea, integritatea și confidențialitatea sistemelor lor. Amenințările împotriva securității cibernetice trebuie luate în serios și prevenite în mod proactiv cu o abordare defensivă la nivel de sistem, specifică nevoilor organizaționale.



The image shows the cover of the ISC2 Research 2025 Cybersecurity Workforce Study. The cover is white with a blue and green design. It features the ISC2 logo at the top, the title '2025 Cybersecurity Workforce Study' in green, and a photograph of three people working together. A hand icon points to the title.

Există o nevoie reală și urgentă de specialiști foarte bine pregătiți în securitate cibernetică, care să poată răspunde eficient noilor amenințări

- conform studiului ISC2, deficitul de competențe eclipsează impactul pe care îl au simplele lipsuri de personal
- AI schimbă regulile jocului în securitatea cibernetică, nu prin înlocuirea oamenilor, ci prin amplificarea competențelor și a modului în care aceștia își desfășoară activitatea
- aproape două treimi dintre respondenți (59%) se confruntă cu nevoi critice sau semnificative de competențe, în creștere față de 44% în 2024

Pe măsură ce **decalajul de competențe în materie de securitate cibernetică continuă să crească** atât în sectorul privat, cât și în cel public, competițiile de securitate cibernetică au fost recunoscute la nivel mondial că o metodă eficientă pentru găsirea de noi talente. Mai mult decât atât, aceste inițiative au fost create pentru a încuraja dezvoltarea competențelor necesare pentru a alege o carieră în securitate cibernetică.

Ce este UNbreakable România?



Despre concurs

UNbreakable România este un concurs național organizat pentru liceeni și studenți din țară ce se pregătesc pentru o carieră în securitate cibernetică sau doresc să-și îmbunătățească cunoștințele din domeniu. La UNbreakable România, participanții vor interacționa cu experți în securitate cibernetică iar la finalul perioadei de pregătire, concurenții își vor putea măsura performanțele din cadrul sezonului, pe parcursul competițiilor pe echipă.

- Concurs național pentru elevi și studenți ce se pregătesc pentru o carieră în securitate cibernetică sau doresc să-și îmbunătățească abilitățile și cunoștințele din domeniu.
- Concept dezvoltat și administrat de companiile ce au coordonat tehnic Campionatul European de Securitate Cibernetică în 2019 la București

Rezultate UNbreakable România 2020-2025

- La concursurile pilot organizate în 2020 s-au înscris peste 500 de participanți (elevi și studenți) ce validează necesitatea unor astfel de activități practice recurente și au fost reprezentate 16 universități și 62 licee din 39 de județe.
- La UNbreakable România în 2021, numărul participanților a fost de aproximativ 1500 din aproape toate județele României. Pentru a consulta în detaliu rezultatele de la edițiile din 2021, puteți accesa [acest infografic](#) (sezonul de primăvară-vară), precum și [acest infografic](#) (sezonul de toamnă-iarnă).

- Ediția din 2022 a UNbreakable România a înregistrat aproape 800 de participanți. Pentru a consulta în detaliu rezultatele ediției, puteți accesa [acest infografic](#).
- Ediția din 2023 a UNbreakable România a înregistrat aproape 900 de participanți. Pentru a consulta în detaliu rezultatele ediției, puteți accesa [acest infografic](#).
- Ediția din 2024 a UNbreakable România a înregistrat peste 1.400 de tineri înscriși. Pentru a consulta în detaliu rezultatele ediției, puteți accesa [acest infografic](#).
- Ediția din 2025 a UNbreakable România a înregistrat peste 1.600 de tineri înscriși. Pentru a consulta în detaliu rezultatele ediției, puteți accesa [acest infografic](#).

Către UNbreakable România 2026

În 2026, UNbreakable România oferă șansa tuturor liceenilor și studenților să participe la concurs și să dezvolte **abilități care să-i pregătească pentru un job în securitate cibernetică**. Performanțele sunt măsurate pe tot parcursul sezonului și competițiile pe echipă acoperă atât dezvoltarea de aptitudini tehnice dar și de soft skills.

În acest an, **programul își îndreaptă atenția mai clar către integrarea inteligenței artificiale în strategii și soluții de securitate**, prin exerciții practice care dezvoltă competențe reale în utilizarea AI pentru cybersecurity și pregătesc participanții să răspundă amenințărilor emergente.

Finala UNbreakable România va avea loc în format fizic și va oferi tinerilor **oportunitatea de a se conecta și de a experimenta spiritul competitiv într-un mod autentic**.

În paralel cu finala va avea loc **Girls in Cyber**, un bootcamp dedicat fetelor cu vârste între 16 și 25 de ani, în cadrul căruia vor fi selectate 20 de participante. **Inițiativa urmărește să inspire mai multe tinere să exploreze domeniul securității cibernetice**, oferindu-le acces la mentorat, ghidare profesională și un cadru în care pot construi conexiuni reale cu alte fete pasionate de acest domeniu.

De asemenea, beneficiul [UNbreakable 24/7/365](#), care oferă participanților acces gratuit la resursele competiției (resurse video, resurse educaționale și laboratoare practice) și în afara perioadelor programului, rămâne disponibil și în acest an. Resursele UNbreakable România sunt și resursele oficiale pentru [Olimpiada de Securitate Cibernetică](#).

Nu în ultimul rând, în ediția 2026, UNbreakable România continuă organizarea unei serii de **competiții locale de tip Capture the Flag** dedicate elevilor de liceu și studenților. Aceste evenimente se vor desfășura în instituții de învățământ selectate, **cu scopul de a-i pregăti pentru competiții naționale de securitate cibernetică** (UNbreakable România, Olimpiada de Securitate Cibernetică, ROCSC2026) și de a **sprijini dezvoltarea unor comunități locale și centre de excelență în domeniu**. Seria de competiții locale va începe odată cu startul noii ediții UNbreakable România și **va continua pe tot parcursul anului în marile orașe ale țării, sub denumirea de Caravana UNbreakable**.

Cui se adresează?



Participarea la evenimentele locale, regionale sau naționale ale evenimentului este gratuită pentru elevi și studenți. Aceștia vor avea oportunitatea de a rezolva exerciții de programare, de apărare cibernetică, incidente și investigații informatice, de a identifica și remedia vulnerabilități din sisteme IT într-un mediu controlat și competitiv.

Participanții pot reprezenta orașul, județul, liceul sau universitatea de care aparțin, iar la finalul fiecărui concurs, partenerii și sponsorii evenimentului îi vor premia pe cei mai buni.

De ce să participi la UNbreakable România?

Inițiativa UNbreakable România a început în 2020 când am organizat concursuri pentru elevi și studenți pasionați de securitate cibernetică. Au fost organizate două competiții în care am avut peste 500 de participanți din aproape 40 de județe ale României.

- Fă un prim pas către o cariera de expert în securitate cibernetică

- Află cum se poziționează echipa ta printre alte echipe formate din colegi, participanți sau prieteni cu aceleași aptitudini - și profită și de ocazia de a-i cunoaște pe ceilalți participanți în cadrul ultimei etape de competiție care va avea loc în format fizic!
- Dezvoltă-ți aptitudinile tehnice și învață lucruri noi
- Rezolvă exerciții inspirate din viața reală, aliniate la standarde internaționale din industrie
- Învață să integrezi tehnologii bazate pe inteligența artificială în procesul de rezolvare a exercițiilor de securitate cibernetică
- Fii pregătit pentru piața muncii: vei învăța să colaborezi, să comunici eficient și să integrezi nativ tehnologiile AI în proiecte organizaționale
- Câștigă premii în bani sau gadget-uri
- Primește diplome de participare sau de câștigător pentru poziția echipei în clasamentul general
- Rezultatul activității echipei tale contribuie la clasamentul [#ROEduCyberSkills](#)
- Obține acces la resursele UNbreakable România prin beneficiul [UNbreakable 24/7/365](#)
- Află care sunt [oportunitățile de studiu](#) al securității cibernetică din România
- Fă parte din comunitatea tânără de securitate cibernetică din România!

Care este programul UNbreakable România și ce se întâmplă în fiecare etapă?



Competiții locale de pregătire

UNbreakable România organizează o serie de competiții locale de tip Capture the Flag (CTF), dedicate elevilor de liceu și studenților.

Aceste evenimente încep înaintea competițiilor de la UNbreakable, cu scopul de a promova securitatea cibernetică în rândul tinerilor și de a-i pregăti pentru competiții naționale de profil.

De asemenea, seria de evenimente locale va continua pe parcursul anului pentru a sprijini dezvoltarea comunităților locale pasionate de securitate cibernetică, sub denumirea de *Caravana UNbreakable*.

Etapa de pregătire și antrenament

Oferă acces gratuit la o serie de resurse și ghiduri dezvoltate prin colaborare între mediul privat și cel academic, pentru dobândirea sau rafinarea cunoștințelor. Pune în legătură participanți cu mentori - experți sau alumni - pe tot parcursul programului de pregătire prin webinarii și grupuri de discuție. **Resursele UNbreakable România sunt utilizate și în pregătirea pentru [Olimpiada de Securitate Cibernetică](#).**

Concursul pe echipe - online

Jocul pe echipe este momentul în care concurezi împreună cu prieteni din școala sau universitatea ta împotriva tuturor celorlalte echipe din UNR. Echipele pot avea maxim 3 membri, așa că poți concura și împotriva altor echipe chiar din școala ta. Performanța din competiția pe echipe este utilizată pentru a calcula clasamentul final #ROEduCyberSkills al echipelor liceelor și universităților din România.

Concursul pe echipe - fizic (finala UNbreakable România)

În funcție de clasamentul final de la concursul online pe echipe, cele mai bune 16 echipe (8 echipe de liceu și 8 echipe de la universitate) vor fi selecționate pentru etapa finală în format fizic. Echipele ce participă la categoria “For Fun” nu sunt eligibile.

Girls in Cyber Bootcamp

În paralel cu finala va avea loc **Girls in Cyber**, un bootcamp dedicat fetelor cu vârste între 16 și 25 de ani, în cadrul căruia vor fi selectate 20 de participante. Inițiativa urmărește să inspire mai multe tinere să exploreze domeniul securității cibernetice, oferindu-le acces la mentorat, ghidare profesională și un cadru în care pot construi conexiuni reale cu alte fete pasionate de acest domeniu.

Misiunea UNbreakable România

Este de a consolida abilitățile strategice și de rezolvare a problemelor și de a le adapta la provocările actuale din securitatea cibernetică și din piața muncii de profil.

Pregătirea participanților pentru UNbreakable România

Care sunt regulile și limitările generale pentru participanți?

- Poți discuta doar cu membrii din echipa ta. Ajutorul din exterior este strict interzis. Exemple de comportament care vor duce la descalificare din concurs: republicarea provocărilor sau a oricărei părți a exercițiilor pe alte website-uri/forumuri, cererea de ajutor sau alterarea provocărilor prin postarea de soluții / flag-uri pe IRC, Stack Overflow, Forumuri, Social Media, Telegram / Whatsapp etc.
- Puteți ataca doar ținte specificate în descrierea exercițiilor.
- Atacarea clasamentului ([acest website](#)) va duce la descalificare.
- Generarea de trafic excesiv nu este permisă (nici măcar dacă intră în obiectivul taskului).
- DOS / DDOS este strict interzis și va aduce cu sine descalificarea din concurs.
- Dacă aveți întrebări despre taskuri și exerciții, întrebați moderatorii pe canalul de discord sau prin email.
- Dacă este prima dată când participi la un astfel de concurs, ar trebui să știi că o soluție (flag) este un cod pe care ar trebui să-l identifici atunci când rezolvi un task. Nu există o procedură standard pentru a le găsi, este recomandat să faci mai multe teste și să nu-ți limitezi gândirea pentru a le obține. În cele din urmă, veți înțelege dinamica acestui tip de concurs CTF și cum să rezolvați rapid provocările.
- Dacă sunteți sigur că ați identificat soluția corectă (flag-ul este 100% corect), dar sistemul nostru nu acceptă să-l transmiteți, informați-ne prin chat.
- Dacă identificați și ne raportați erori în infrastructura de concurs, puteți fi recompensați.
- Avem un clasament dinamic, ceea ce înseamnă că, cu cât mai multe echipe rezolvă o provocare, cu atât punctajul problemei scade.
- **Rezolvarea probelor cu ajutorul inteligenței artificiale este tolerată în faza online, unde scopul principal este explorarea problemelor și a abordărilor posibile.**
- **În faza finală, utilizarea AI este, în principiu, interzisă, competiția concentrându-se pe:**
 - gândire proprie și raționament tehnic;
 - capacitatea reală de analiză și rezolvare a problemelor;
 - evaluarea corectă a competențelor participanților.
- **Prin excepție, în faza finală vor exista probe marcate explicit în care utilizarea AI este permisă, acestea fiind concepute special pentru a evalua:**
 - modul de folosire responsabilă și eficientă a AI;
 - capacitatea de a formula cerințe (prompting) și de a valida rezultatele;
 - integrarea AI ca instrument de lucru, nu ca substitut al competenței tehnice.
- Puteți găsi cele mai recente știri și anunțuri despre acest concurs pe [pagina de știri](#).

Mai multe detalii despre regulament puteți găsi pe pagina de întrebări comune și regulament: <https://unbreakable.ro/regulament>

Care sunt și cum se calculează criteriile de evaluare?

Principalul obiectiv al UNbreakable România este de a încuraja tinerii să participe la competiții de securitate cibernetică pentru a se pregăti eficient pentru un viitor loc de muncă în domeniu.

Un alt obiectiv important este crearea unui mecanism de evaluare pentru aceștia. Fiecare sezon are mai multe etape de concurs. Fiecare etapă de concurs are un clasament dedicat. Fiecare etapă are mai multe exerciții.



Nivelul de dificultate al exercițiilor

Fiecare etapă va avea aproximativ 80% din totalul de exerciții cu dificultate ușoară spre medie și mai puțin de 20% din exerciții vor avea o dificultate ridicată.

Scorul pe etapă

Scorul pe etapă pentru rezolvarea unui exercițiu se calculează prin adunarea tuturor punctelor obținute după rezolvarea exercițiilor propuse de organizatori sau prin răspunderea corectă la întrebările teoretice din perioada etapei.

Clasamentul pe etapă poate fi influențat de:

- totalul punctelor obținute prin rezolvarea exercițiilor
- acuratețea sau numărul de încercări folosite pentru a rezolva un exercițiu
- timpul ultimului exercițiu sau întrebare rezolvată corect

Suplimentar, fiecare echipa ce a obținut puncte va fi încadrat în una din categoriile următoare în fiecare etapă:

- Gold - Top 15% echipe
- Silver - Top 15-35% echipe
- Bronze - Top 35-50% echipe

Punctajul unui exercițiu - exerciții de tip Jeopardy

Modalitatea de calcul pentru punctele primite alocate fiecărui exercițiu de tip Jeopardy este anunțată înainte de rezolvarea acestuia și poate fi de două feluri:

- punctaj fix - fiecare întrebare are un număr exact de puncte, știut în avans
- punctaj dinamic - fiecare întrebare are un punctaj fix inițial, iar valoarea răspunsului corect scade odată cu numărul de rezolvări ale aceluși exercițiu pentru toți jucătorii, după formula:

```
scorExercitiu = min(  
    max(valoareInitiala * 0.1, valoareInitiala - ((valoareInitiala / numarMaximJucatori) *  
totalRezolvari)),  
    valoareInitiala  
)
```

unde:

- valoareInitiala este totalul de puncte inițial pentru orice exercițiu, în general este 500 de puncte
- numarMaximJucatori este numărul maxim de jucători ce trebuie să rezolve un exercițiu pentru a atinge valoarea minimă
- totalRezolvari este numărul total de jucători ce au rezolvat un exercițiu

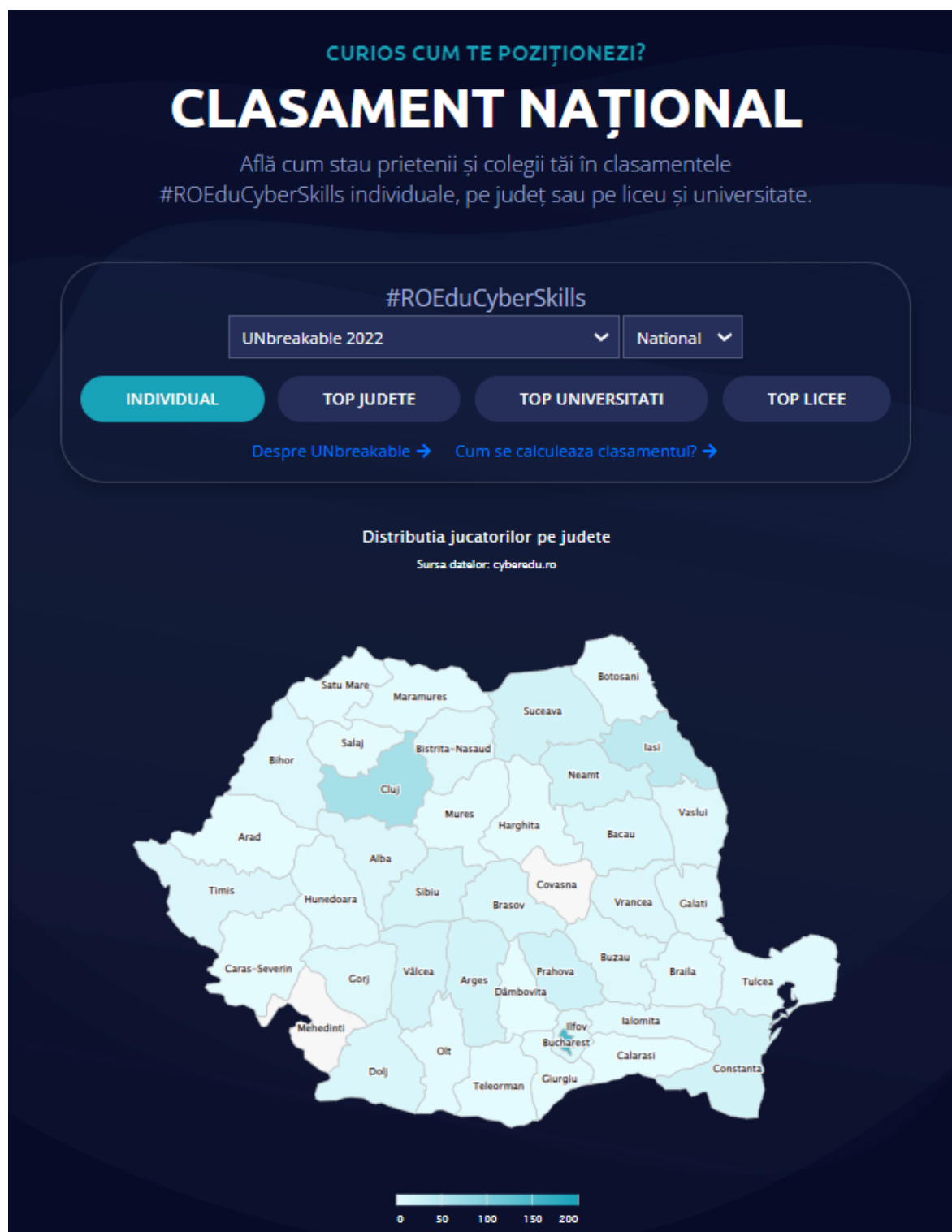
Scorul pe sezon

Scorul final pe sezon ia în considerare scorurile agregate din fiecare etapă de concurs. Scorul pe sezon va prezenta rezultatele obținute pentru fiecare etapă.

Clasamentul pe etapă poate fi influențat de:

- totalul punctelor obținute prin rezolvarea exercițiilor
- acuratețea sau numărul de încercări folosite pentru a rezolva un exercițiu
- timpul ultimului exercițiu sau întrebare rezolvată corect

Ce înseamnă clasamentul pe județ, liceu sau universitate - #ROEduCyberSkills



Fiecare județ, liceu sau universitate reprezentată va avea o poziție în clasamentul #ROEduCyberSkills pentru fiecare etapă, urmărindu-se următoarele aspecte:

- cea mai bine clasată echipă din etapa pe echipe (online)
- clasamentul pentru etapa fizică (etapa finală)
- număr total de echipe înregistrate ce au obținut punctaj mai mare de 0 la etapa online
- punctajul mediu pentru echipele ce au obținut punctaj mai mare de 0 la etapa online

O echipă poate contribui la #ROEduCyberSkills prin înregistrare și participare la etapa online, menționând instituția de învățământ de care aparține.

O echipă poate contribui la #ROEduCyberSkills prin participarea cu minim 1 jucător și maxim 3 jucători cu respectarea regulamentului privind formarea echipelor.

Care sunt grupele în care poate fi încadrată o echipă?

Fiecare echipă poate fi încadrată în una din grupele:

- **High School Student în România**, echipe cu tineri peste 16 ani ce sunt înscriși la un liceu din România
- **College / University in Romania**, studenți înscriși la o universitate din România
- **For fun**, deschis pentru oricine

Cum se poate pregăti un participant pentru UNbreakable România?

UNbreakable România debutează cu o serie de competiții de tip CTF organizate în marile orașe din țară. Tinerii își vor testa abilitățile și vor învăța cum se desfășoară o competiție de securitate cibernetică în cadrul unui concurs de aproximativ 6 ore, de dificultate ușoară spre medie.

Apoi, pe parcursul etapei de antrenament și pregătire, participanții vor avea la dispoziție, pe platforma [CyberEDU](#), resurse teoretice și practice ce le va permite familiarizarea cu formatul și metodologia concursului.



Platforma CyberEDU a fost utilizată în toate etapele UNbreakable Romania, dar și în competiții precum Olimpiada de Securitate Cibernetică (OSC), Campionatul Național de Securitate Cibernetică (ROCSC), precum și în procesul de selecție a lotului național care va reprezenta România la ECSC.

Liceenii și studenții au la dispoziție secțiunea UNbreakable România de pe platforma [CyberEDU](#), accesibilă prin crearea unui cont.

Secțiunea UNbreakable include:

- **Trainings** - cursuri teoretice pentru aprofundarea conceptelor de securitate cibernetică
- **Challenges** - exerciții practice din sezoanele precedente ale UNbreakable România

Accesul la secțiunea UNbreakable România se face prin înregistrarea pe platforma CyberEDU și înscrierea la UNbreakable Romania 2026, folosind [acest link](#).

De asemenea, pe parcursul etapei de pregătire se vor organiza webinarii cu experți în securitate cibernetică sau alumni din comunitate pe diverse subiecte de interes.

La UNbreakable, subiectele vor trata unul sau mai multe concepte din categoriile de mai jos. Întrebările și exercițiile propuse vor atinge atât concepte teoretice cât și aspecte practice ale fiecărei categorii.

Pentru a acoperi metodologia, fiecare participant înscris va primi în etapa de pregătire, pe platforma [CyberEDU](#), resurse teoretice și exemple de exerciții practice ca să înțeleagă conceptele și să se familiarizeze cu modelul de concurs. Mai mult decât atât, tot în această etapă, liceenii și studenții vor avea acces la o serie de mentori care vor organiza sesiuni de discuții și webinarii.

Scopul etapei de pregătire este de a da oportunitatea tuturor să se implice în acest tip de competiție, chiar dacă nu au experiență dar își doresc să se dezvolte în securitate cibernetică.

Exercițiile sunt organizate sub forma unui concurs de tip „Capture the Flag”, incluzând întrebări cu una sau mai multe variante de răspuns, precum și probe practice de tip „Jeopardy” și „Attack & Defence”. Tematicile acoperite sunt variate și reflectă atât concepte introductive, cât și aspecte avansate din domeniul securității cibernetică, după cum urmează:

1. Tematici generale (introductive și teoretice)

- Concepte fundamentale de securitate cibernetică
- Tehnologii și mecanisme de protecție (firewall, IDS/IPS, EDR, MFA etc.)
- Tehnologii pentru identificarea vulnerabilităților și gestionarea patch-urilor
- Tehnologii și metode de anonimizare și protejare a identității online
- Tehnici de inginerie socială și prevenirea acestora
- Securitatea și managementul parolelor, bune practici și politici
- Participarea la programe de tip bug bounty și procesul de responsible disclosure
- Elemente introductive privind dezvoltarea unui business sau startup în domeniul securității
- Concepte fundamentale de guvernanță, managementul riscului și conformitate (GRC)

2. Tematici tehnice (practici și avansate)

- Criptografie, algoritmi de criptare, encodare și hashing
- Securitatea și exploatarea vulnerabilităților în aplicații web
- Securitatea și exploatarea vulnerabilităților în aplicații mobile și desktop
- Investigații cu tehnici OSINT (Open Source Intelligence)
- Enumerarea și exploatarea serviciilor, sistemelor și rețelelor
- Analiza jurnalelor electronice (logs) și corelarea lor pentru identificarea incidentelor
- Analiza traficului de rețea și identificarea anomaliilor
- Analiza capturilor de date, memorie sau hard disk (forensics digital)
- Inginerie inversă pentru aplicații executabile, scripturi sau documente
- Securitatea rețelelor wireless și identificarea vulnerabilităților specifice
- Auditul codului sursă și identificarea erorilor de implementare
- Configurarea și securizarea sistemelor de operare, serviciilor și infrastructurilor
- Programare și scripting (Python, Bash etc.) pentru automatizarea rezolvării exercițiilor
- Inteligența artificială

3. Tematici specifice pentru exercițiile de tip „Attack & Defence”

- Dezvoltarea și implementarea mecanismelor defensive pentru protejarea unui sistem sau a unei rețele
- Monitorizarea sistemelor pentru identificarea semnelor unui atac sau incident
- Identificarea, exploatarea și remedierea vulnerabilităților în servicii și aplicații expuse
- Hardening, patching, detectare și răspuns în timp real
- Strategii de continuitate operațională în contextul atacurilor adversarilor

4. Alte arii conexe

- Elemente de programare avansată aplicate în contexte de securitate
- Noțiuni generale și specializate privind securitatea sistemelor informatice
- Exerciții inter-disciplinare ce combină mai multe arii tehnice sau teoretice

Care sunt oportunitățile de dezvoltare în afară de UNbreakable România pentru elevi și studenți?

Domeniul securității cibernetice este extrem de vast și există numeroase oportunități pentru a urma o carieră în industrie, precum:

- **Penetration Tester** - Specialist în securitate informatică responsabil cu identificarea vulnerabilităților în sisteme informatice folosind tehnici cunoscute de hackeri
- **Analist în Securitate** - Specialist responsabil cu monitorizarea și detectarea atacurilor informatice
- **Specialist în răspunsul la incidente de securitate**
- **Specialist în investigarea atacurilor informatice**
- **Specialist în analiza aplicațiilor malware**

În România se organizează mai multe competiții de tip Capture the Flag, printre care amintim:

- Olimpiada de Securitate Cibernetică - <https://osc.rocsc.ro/>
- Campionatul European de Securitate Cibernetică - <https://www.cybersecuritychallenge.ro/>
- DefCamp Capture the Flag - <https://def.camp>
- HackTM - hacktm.ro/
- TFC CTF - <https://ctftime.org/ctf/696/>
- Anual, pe platforma <https://cyber-edu.co/>, sunt anunțate și organizate și alte evenimente.

Pentru a urmări calendarul internațional de concursuri, puteți accesa portalul <https://ctftime.org/>.

Care sunt resursele necesare pentru a putea participa la competiții?

Fiecare competiție are specificul ei, în general cunoștințele ating mai multe subiecte, printre care:

- Cunoștințe avansate de programare în diverse limbaje de programare (eg. python, c/c++, php, nodejs, asm etc.)
- Cunoștințe despre vulnerabilități și exploatarea lor
- Cunoștințe despre investigarea traficului, a capturilor de memorie sau de disc
- Cunoștințe de criptografie
- Cunoștințe despre sisteme informatice și rețele
- Cunoștințe despre aplicații mobile, desktop sau web

La UNbreakable, în etapa de pregătire, participanții vor primi o serie de resurse și exemple de exerciții rezolvate și vor avea posibilitatea să participe la webinarii organizate de mentorii evenimentului.

Cum pot adresa întrebări Organizatorilor sau Mentorilor?

Ne puteți lăsa un scurt mesaj [pe pagina de contact](#) sau direct la adresa [contact@\[@\]cyber-edu\[.\]co](mailto:contact@[@]cyber-edu[.]co) pentru a intra în legătură cu organizatorii evenimentului.

Mentorii vor fi disponibili în timpul webinarilor sau pe canalele Discord oficiale ale acestui eveniment.

Pregătire antrenori și profesori pentru UNbreakable România



Care este rolul unui antrenor sau profesor?

UNbreakable România este conceput pentru a încuraja implicarea activă a mediului academic în fiecare sezon al competiției. Profesorii și antrenorii au un rol esențial în ghidarea și motivarea elevilor și studenților pasionați de securitate cibernetică.

Organizatorii pun la dispoziția acestora resurse și instrumente dedicate, precum **Ghidul profesorului/antrenorului UNR**, dar și oportunități de comunicare și colaborare cu experți și alumni din domeniu, pentru alinierea activităților educaționale la standardele internaționale din industrie. Obiectivul este sprijinirea procesului de pregătire a participanților prin platforma educațională [CyberEDU](#).

Pentru ca un liceu sau o universitate să participe la **UNbreakable România**, este nevoie de elevi sau studenți entuziaști, interesați de securitate cibernetică, o conexiune la internet și un calculator cu performanțe obișnuite.

Rolul profesorului/antrenorului este de a:

- încuraja elevii și studenții să se înscrie în competiție;
- disemina mesajele și resursele UNbreakable România în comunitatea academică;
- lucra cu participanții, folosind una dintre cele două opțiuni de pregătire:

1. UNbreakable România 24/7/365

Participanții **UNbreakable România** și-au dorit mereu acces gratuit la resursele competiției (resurse video, resurse educaționale și laboratoare practice), inclusiv în afara perioadelor oficiale ale competiției.

Pentru a veni în sprijinul lor, a fost lansat beneficiul „UNbreakable România 24/7/365”. Orice instituție academică - universitate, liceu sau centru de excelență în securitate cibernetică din România - care se înregistrează în acest program are posibilitatea:

- să acceseze **gratuit resursele competiției** (resurse video, resurse educaționale și laboratoare practice) pe tot parcursul anului, pentru toți elevii și studenții;
- să **beneficieze de un spațiu dedicat** pe platforma CyberEDU, unde elevii și studenții pot accesa peste **200 de laboratoare gratuite**;
- să **organizeze concursuri private** cu colegii lor, direct pe platforma CyberEDU.

Vă puteți înregistra la UNbreakable România accesând [acest link](#).

2. Classrooms

Classrooms este o nouă funcționalitate dezvoltată pe platforma CyberEDU care permite profesorilor să:

- organizeze cu ușurință grupe de elevi sau studenți
- atribuie cursuri și laboratoare potrivite ritmului și parcursului de învățare al fiecărui cursant
- urmărește activitatea, rezultatele și progresul fiecărei grupe sau al fiecărui elev/student
- identifică rapid subiectele care au nevoie de mai multă atenție sau aprofundare, pe baza progresului real
- ajustează planul de învățare acolo unde este necesar

Astfel, profesorii devin facilitatori ai procesului de învățare și mentori care sprijină dezvoltarea viitorilor specialiști în securitate cibernetică.

Cum mă pot înscrie ca antrenor sau profesor pentru a reprezenta o instituție de învățământ?

În acest moment nu este necesară înscrierea unui antrenor sau profesor pe platformă. În momentul în care se înscriu la UNbreakable România, participanții pot menționa numele și adresa de email a profesorului ce îi reprezintă.

Cum pot urmări activitatea participanților pe parcursul programului UNbreakable România?

- Clasamentul #ROEduCyberSkills poate fi urmărit direct pe site-ul oficial pe adresa: <https://unbreakable.ro/clasament>
- Fiecare etapă a concursului va avea o pagina unică pe platforma <https://cyber-edu.co/> de unde puteți vedea rezultatele și activitatea participanților în timp real. Aceste pagini pentru eveniment vor fi comunicate în prealabil.

Cum se vor alcătui echipele?

La concursul pe echipe, participanții trebuie să formeze echipe cu alți colegi din unitatea de învățământ de care aparțin. O echipă poate avea maxim 3 membri, iar aceștia trebuie să fie din aceeași unitate de învățământ. Cei care nu reușesc să se alăture unei echipe din școala/unitatea de învățământ vor fi adăugați automat într-o echipă din altă unitate de învățământ sau pot alege să participe individual dacă nu pot găsi alți membri. Obiectivul este rezolvarea a cât mai multe exerciții în timpul alocat.

Cum vor fi selecționați finaliștii pentru faza finală?

Cele mai bune 16 echipe (8 echipe din cadrul universităților și 8 echipe de liceu) vor fi selecționate pentru etapa finală în format fizic, în funcție de clasamentul final de la concursul online pe echipe.

Echipele ce participă la categoria “For Fun” nu sunt eligibile.

Exemple de exerciții

Care sunt tipurile de exerciții?

Tipuri de exerciții

- exerciții teoretice, cu răspuns închis
- exerciții teoretice, cu variante de răspuns
- exerciții practice de tip Capture the Flag (Jeopardy), cu răspuns închis

Nivelul de dificultate al exercițiilor

Fiecare etapă va avea aproximativ 80% din totalul de exerciții cu dificultate ușoară spre medie și mai puțin de 20% din exerciții vor avea o dificultate ridicată.

Cum arata un flag / steag?

Formatul unui flag / steag va fi anunțat pentru fiecare exercițiu. Acesta poate avea mai multe forme, spre exemplu:

- Răspuns cu format non-standard: de eg. Ubuntu 20.04
- Răspuns în format CTF{sha256}: de eg.
CTF{9c9611ed839c917b34355ce5523c02aa8f6fa1c21f873ae6b8eb69fe1c83fa6c}
- Răspuns în format UNR{alfanumeric}: UNR{felicitari-ai-raspuns-corect}

Cum pot obține un flag / steag?

În cazul unui exercițiu teoretic, răspunsul corect poate fi obținut prin răspunderea corectă la o serie de întrebări cu răspuns închis sau variante de răspuns.

În cazul unui exercițiu practic, răspunsul corect (flag standard sau non-standard) poate fi obținut prin rezolvarea corectă a exercițiului propus de către organizatori, în funcție de tipul exercițiului. Cu titlul de exemplu:

- Identificarea și exploatarea unei vulnerabilități într-o aplicație web
- Identificarea și exploatarea unei vulnerabilități dintr-o aplicație de tip serviciu
- Identificarea răspunsului corect într-o captură de date (eg. captura de memorie, loguri, fișiere etc.)
- Recuperarea răspunsului prin crearea unui algoritm de decriptare sau exploatare a unei vulnerabilități într-un algoritm criptografic simplu
- Aplicarea unor tehnici de recuperare a codului sursă pentru a identifica vulnerabilități
- Evaluarea codului sursă al unei aplicații și dezvoltarea unei tehnici ce permite abuzarea funcționalităților existente, etc.

Cum arată un exercițiu teoretic?

Exemplu exercițiu teoretic #1

Nivel de dificultate:

începător

Întrebare

Care este portul standard folosit pentru protocoale ssh?

Răspuns

22

Exemplu exercițiu teoretic #2

Nivel de dificultate:

începător - ușor

Întrebare

Ce algoritm de encodare este folosit în linia de cod de mai jos?

```
a_list = [chr(ord(a) ^ ord(b)) for a,b in zip(randA, randB)]
```

Răspuns

xor

Cum arată un exercițiu practic?

Exemplu exercițiu practic #1

Nivel de dificultate:

începător - ușor

Descriere:

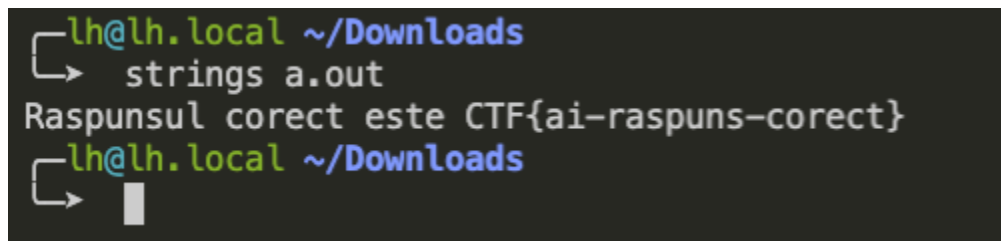
Un programator a dezvoltat o aplicație în limbajul de programare C/C++ în care a ascuns un mesaj secret. În documentul atașat găsiți aplicația deja compilată, fără acces la codul sursă.

Obiectivul este să recuperați mesajul secret.

Mod de rezolvare:

Există numeroase aplicații cu ajutorul cărora poți decompila o aplicație scrisă în C/C++, însă pentru acest exercițiu poți rula un utilitar comun pe sistemele de operare Linux.

Comanda rulată: *strings nume_fisier*.



```
lh@lh.local ~/Downloads
└─ strings a.out
Raspunsul corect este CTF{ai-raspuns-corect}
lh@lh.local ~/Downloads
└─
```

Răspuns corect:

CTF{ai-raspuns-corect}

Exemplu exercițiu practic #2

Nivel de dificultate:

Ușor - mediu

Descriere:

Steve Kobbs este specialist în meteorologie.

A fost chemat să-și ofere expertiza cu privire la ultimul tsunami care a avut loc în țara noastră.

În timp ce Steve lucra, un pachet misterios a ajuns la ușă.

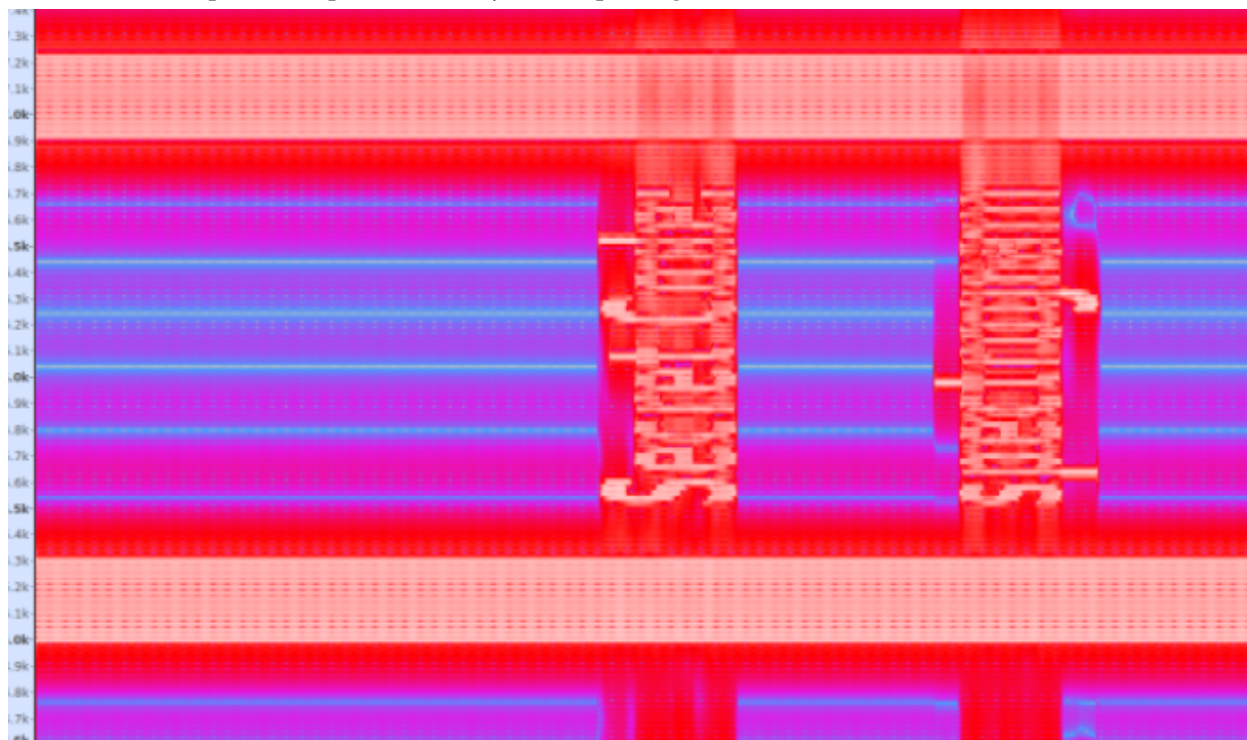
În interior, a fost găsit un stick USB, care conținea următorul fișier audio: rain.wav

Formatul semnalizării: răspunsul corect este în text simplu și trebuie trimis jucătorilor sub forma `ctf{sha256 a cuvântului în text clar}`.

Scop: Utilizați diverse tehnici pentru a analiza fișierele audio pentru a recupera pavilionul care este ascuns în fișierul `rain.wav`.

Mod de rezolvare:

După ce încerci mai multe programe de steganografie, soluția s-a dovedit a fi destul de simplă. Deschizi fișierul `rain.wav` în Audacity și schimbi modul de vizualizare în ‘Spectrogram’. Deschizi apoi meniul Setări spectrogramă și încerci mai multe numere pentru dimensiunea ferestrei, stabilindu-se în cele din urmă la 4096. După ce faci puțin zoom, așa arăta spectrograma:



Sursa fotografiei: blog.kuhi.to

Răspunsul corect:

În cazul în care nu îl puteți vedea, graficul arată „Cod secret: “spectrogram”.

Flagul este `ctf{sha256(spectrogram)}`.

Folosind un tool precum acesta: <https://emn178.github.io/online-tools/sha256.html>, veți obține: `ctf{cc3a329919391e291f0a41b7afd3877546f70813f0c06a8454912e0a92099369}` care este și răspunsul corect.

Ce sistem de operare ar trebui folosit în timpul concursului?

Recomandăm utilizarea unui sistem de operare cu care participanții sunt obișnuiți. Pentru eficiență, recomandăm existența unei mașini virtuale cu un sistem de operare de tip Linux, cum ar fi Ubuntu / Debian și familiarizarea cu acesta înainte de concurs.

Specialiștii în securitate informatică mai folosesc Kali Linux sau Parrot ca sisteme de operare ce au preinstalate diverse unelte ce îi pot asista în rezolvarea exercițiilor.

Implicare și suport

Cum pot deveni mentor?

Ce înseamnă mentorat?

Mentoratul este o relație de învățare, axată în general pe dezvoltarea carierei pe termen lung a unei persoane care primește sprijin de la o persoană cu experiență. Scopul principal este acela de a stimula creșterea personală și profesională, dezvoltarea abilităților, cunoștințelor și înțelegerii unui anumit domeniu, în cazul nostru în securitate cibernetică.

Ce rol au mentorii?

Mentorii de la UNbreakable au un rol foarte important care acoperă în principiu nevoia de suport și susținere pentru noua generație de specialiști în securitate informatică din România. Aceștia vor răspunde la întrebările participanților în etapa de pregătire, se vor implica în webinarii și vor participa activ în dezvoltarea programei de exerciții pentru sezonul în curs.

Responsabilitatea unui mentor

- propune sau contribuie la îmbunătățirea resurselor existente, a programei concursului
- propune exerciții
- organizează webinarii pentru jucători pe diverse subiecte, pentru dezvoltarea abilităților tehnice și soft
- răspunde la întrebări pe canalele de discuții UNbreakable

Mai multe despre mentori aici: <https://unbreakable.ro/mentori>

Cum poate instituția noastră să devină partener al evenimentului?

Care sunt principalele beneficii de participare pentru un liceu sau o universitate?

- încurajarea dezvoltării abilităților studenților prin participarea la o competiție națională
- promovarea programelor de studii din instituția de învățământ
- evaluarea studenților și posibilitatea de a urmări evoluția acestora
- prestigiu și recunoaștere națională
- posibilitatea de a contribui la adaptarea curriculei și exercițiilor din programa evenimentului
- oportunități de colaborare între instituții
- dezvoltarea unor comunități locale sau a unor centre de excelență în securitate cibernetică

Cum se poate implica un liceu sau o universitate?

- încurajează participarea elevilor și studenților la concurs - accesul este gratuit
- identifică profesorii potriviți ce ar putea deveni antrenori pentru participanți
- susțin elevii sau studenții dvs. cu sfaturi și resurse pentru a-și dezvolta cunoștințele și abilitățile tehnice și non-tehnice ce îi vor ajuta să obțină rezultate bune la concurs
- propune exerciții pentru toate etapele concursului
- propune un expert sau un alumni pentru a fi mentor în concurs
- se asigură că jucătorii respectă regulile impuse de organizatori
- se asigură că jucătorii participă în toate etapele de sezon
- pot oferi suport logistic în organizarea competiției în format fizic
- înregistrează cursurile sau programele de master / doctorat în securitate cibernetică pentru ca tinerii să poată vedea ce [oportunități de studiu](#) în domeniu există în România
- organizează evenimente locale de pregătire, pe tot parcursul anului, în cadrul inițiativei *Caravana UNbreakable*
- se înregistrează în [UNbreakable 24/7/365](#), pentru ca elevii / studenții să aibă acces la toate resursele UNbreakable, chiar și în afara perioadei de pregătire
- activează funcționalitatea CLASSROOMS, care permite:
 - organizarea de grupe de elevi / studenți
 - atribuirea de cursuri și laboratoare potrivite ritmului și parcursului de învățare al fiecărui cursant
 - urmărirea activității, rezultatele și progresul fiecărei grupe sau a fiecărui elev/student
 - identificarea rapidă a subiectelor care au nevoie de mai multă atenție sau aprofundare, pe baza progresului real
 - ajustarea planului de învățare acolo unde este necesar

Cum pot fi susținuți studenții?

- identificați și accesați surse de finanțare pentru burse, cursuri speciale și laboratoare practice

- includeți sezoanele UNbreakable ca parte din activitățile lor de la școală
- programați sesiuni de practică pe diverse subiecte din [materia](#) concursului
- creați laboratoare de practica sau recomandați înscrierea pe platforma educațională CyberEDU.ro
- oferiți-le sfaturi practice pentru o carieră în securitate cibernetică
- oferă posibilitatea liceenilor / studenților lor să aibă acces la toate resursele UNbreakable, chiar și în afara perioadei de pregătire, prin programul [UNbreakable 24/7/365](#)

Ce resurse sunt disponibile pentru a-i pregăti pe studenți?

- studenții înscriși în program vor primi, pe platforma [CyberEDU](#), un pachet de referințe și resurse pentru a se pregăti în etapa de antrenament; aceste resurse vor fi utilizate și în pregătirea pentru [Olimpiada de Securitate Cibernetică](#)
- profesorii au la dispoziție un ghid ce răspunde la principalele întrebări despre cum funcționează concursul, dar care conține și exemple de exerciții
- organizează sesiuni de pregătire practică pe platforma CyberEDU, organizatorii UNbreakable putând să vă pună la dispoziție funcționalități ce permit realizarea unor sesiuni de tip examen cu aceștia
- vedeți [aici](#) exercițiile date de organizatori la concursului pilot din 2020, iar în perioada de Bootcamp participanții vor avea acces la toate exercițiile din 2020 și până la ediția din 2025, inclusiv cu exemplu de rezolvare
- [flyer-ul](#) concursului pe care îl puteți distribui și altor persoane interesate
- Pe [canalul de Youtube](#) veți găsi resurse video pentru webinarile susținute de experți și mentori la edițiile anterioare

Cum pot contribui la dezvoltarea resurselor pentru participanți?

Ne puteți lăsa un scurt mesaj [pe pagina de contact](#) sau direct la adresa [contact\[@\]cyber-edu\[.\]co](mailto:contact[@]cyber-edu[.]co).

Cum poți contacta organizatorii?

Dacă ai orice întrebare despre regulamentul concursului, următoarele etape sau doar vrei să ne saluți, folosește cu încredere următorul formular iar unul dintre colegii noștri îți va răspunde cât se poate de repede!

Ne puteți lăsa un scurt mesaj [pe pagina de contact](#) sau direct la adresa [contact\[@\]cyber-edu\[.\]co](mailto:contact[@]cyber-edu[.]co).