



Introducere in securitate cibernetica

Resurse utile pentru incepatori din UNbreakable România

unbreakable.ro

Declinarea responsabilității	5
Introducere	6
Tehnologii pentru asigurarea securității cibernetică	7
Ce este asigurarea și securitatea informației?	7
Ce sunt controalele de securitate cibernetică?	7
Obiectivele controalelor de securitate cibernetică	7
Clasificarea controalelor de securitate cibernetică	8
A. După tip	8
A.1 Controlul Tehnic	8
A.2 Controlul Administrativ	9
A.3 Controlul Operațional	9
A.4 Controlul Fizic	9
B. După funcție	10
B.1 Preventiv	10
B.2 Controlul Compensator	10
B.3 Controlul corectiv	11
B.4 Controlul Detectiv	11
B.5 Controlul Descurajator	11
Tehnologii pentru identificarea vulnerabilităților	12
Ce este o vulnerabilitate?	12
Ce reprezintă un proces de identificare / detecție a vulnerabilităților?	12
Categorii de procese de identificare a vulnerabilităților	12
Etapile unui proces de identificare a vulnerabilităților	13
Tehnologii folosite în identificarea manuală și automată a vulnerabilităților	14
Tehnologii de anonimizare	15
Ce este un proces de anonimizare a datelor?	15
Tehnici de anonimizare a datelor	15
Avantajele unui proces de anonimizare a datelor	16
Tehnologii utilizate în procesul de anonimizare a datelor	16
Atacuri și tehnici de inginerie socială	17
Ce sunt atacurile și tehnicile de inginerie socială?	17
Care sunt pașii unui atac de inginerie socială?	17
Tehnici de atacuri de inginerie socială	17
Baiting	18

Scareware	18
Pretexting	19
Phishing	19
Spear phishing	19
Metode de prevenire a atacurilor de inginerie socială	20
Managementul parolelor și tehnici de spargere parolelor	20
Ce este managementul parolelor?	20
Ce provocări sunt întâlnite în gestionarea parolelor?	20
Ce metode de protecție putem folosi împotriva acestor atacuri?	21
Participarea la programe de tip bug bounty	21
Ce este un program de tip bug bounty?	21
Cine apelează la programele de tip bug bounty?	22
De ce companiile optează pentru programele de tip bounty?	22
De ce participă cercetătorii și specialiștii în domeniu participă la programele bug bounty?	22
Platforme ce oferă programe de tip bug bounty	22
Dezvoltarea unui business sau startup în securitate cibernetică	23
Ce este un Startup?	23
Care sunt etapele de dezvoltare prin care trece un startup?	23
Găsirea ideii	23
Formarea echipei	24
Testarea pieței	24
Crearea unui prototip	24
Dezvoltarea modelului de business	25
Dezvoltarea strategiei de marketing	26
Atragerea unor finanțări	26
Scalarea	27
Strategia de exit	27
Startup-uri românești de securitate	28
Pentest Tools	28
Dekeneas	28
Appsulate	29
TypingDNA	29
Bit Sentinel	30
CyberEDU	30
Pregătire pentru UNbreakable România	31
Care sunt regulile și limitările generale pentru participanți?	31
Care sunt și cum se calculează criteriile de evaluare?	32

Nivelul de dificultate al exercițiilor	32
Scorul pe etapă	32
Punctajul unui exercițiu	33
Scorul pe sezon	33
Ce înseamnă clasamentul pe județ, liceu sau universitate - #ROEduCyberSkills	34
Ce este raportul individual de performanță?	35
Care sunt grupele în care poate fi încadrat un participant?	35
Cum se poate pregăti un participant pentru UNbreakable România?	36
Care sunt oportunitățile de dezvoltare în afara de UNbreakable Romania pentru elevi și studenți?	37
Care sunt resursele necesare pentru a putea participa la competiții?	38
Exerciții și rezolvări	38
Warm-UP Individual	38
Social-Agency (Hard)	41
Basic-ics (easy)	43
Eyewitness (mediu)	54
Rise (ușor)	56
Contribuitori	57

Declinarea responsabilității

Aceste materiale și resurse sunt destinate exclusiv informării și discuțiilor, având ca obiectiv conștientizarea riscurilor și amenințărilor informatice dar și pregătirea unor noi generații de specialiști în securitate informatică.

Organizatorii și partenerii UNbreakable România nu oferă nicio garanție de niciun fel cu privire la aceste informații. În niciun caz, organizatorii și partenerii UNbreakable România, sau contractanții, sau subcontractanții săi nu vor fi răspunzători pentru niciun fel de daune, inclusiv, dar fără a se limita la, daune directe, indirecte, speciale sau ulterioare, care rezultă din orice mod ce are legătură cu aceste informații, indiferent dacă se bazează sau nu pe garanție, contract, delict sau altfel, indiferent dacă este sau nu din neglijență și dacă vătămarea a fost sau nu rezultată din rezultatele sau dependența de informații.

Organizatorii UNbreakable România nu aprobă niciun produs sau serviciu comercial, inclusiv subiectele analizei. Orice referire la produse comerciale, procese sau servicii specifice prin marca de servicii, marca comercială, producător sau altfel, nu constituie sau implică aprobarea, recomandarea sau favorizarea acestora de către UNbreakable România.

Organizatorii UNbreakable România recomandă folosirea cunoștințelor și tehnologiilor prezentate în aceste resurse doar în scop educațional sau profesional pe calculatoare, site-uri, servere, servicii sau alte sisteme informatice doar după obținerea acordului explicit în prealabil din partea proprietarilor.

Utilizarea unor tehnici sau unelte prezentate în aceste materiale împotriva unor sisteme informatice, fără acordul proprietarilor, poate fi considerată infracțiune în diverse țări.

În România, accesul ilegal la un sistem informatic este considerată infracțiune contra siguranței și integrității sistemelor și datelor informatice și poate fi pedepsită conform legii.

Introducere

Securitatea cibernetică este practica securizării rețelelor, a sistemelor și a oricărei alte infrastructuri digitale împotriva atacurilor ciberneticе. Băncile, companiile de tehnologie, spitalele, agențiile guvernamentale și aproape orice alta industrie cu o componenta digitală investesc în infrastructura de securitate cibernetică pentru a-și proteja practicile comerciale și milioanele de clienți cu care au încredere datele lor.

Securitatea cibernetică este vitală deoarece are legătură directă cu protejarea datelor noastre sensibile, a informațiilor de identificare personală (PII), a informațiilor de sănătate protejate (PHI), a datelor personale, a proprietății intelectuale, a datelor și a sistemelor de informații guvernamentale și din industrie împotriva furtului și daunelor încercate de infractori ciberneticі.

Mai mult decât atât, importanța securității ciberneticе este în continua creștere. În esență, societatea noastră depinde mai mult din punct de vedere tehnologic decât oricând și nu există niciun semn că această tendință va încetini în viitor. Bresele de securitate și pierderile de date care ar putea duce la furtul de identitate sunt acum postate public pe conturile de socializare. Informațiile sensibile, cum ar fi datele personale, informațiile despre cardul de credit și detaliile contului bancar sunt acum stocate în servicii de stocare în cloud, cum ar fi Dropbox sau Google Drive.

Faptul este că sunteți o persoană fizică, o companie sau o multinațională, vă bazați în fiecare zi pe sisteme informatice. Adăugați acest lucru cu creșterea serviciilor de tip cloud, securitatea slabă a serviciilor cloud, smartphone-urile și Internet of Things (IoT) și avem o multitudine de amenințări la adresa securității ciberneticе care nu existau acum câteva decenii. Trebuie să înțelegem diferența dintre securitatea cibernetică și securitatea informațiilor, chiar dacă abilitățile devin mai similare.

Securitatea cibernetică nu a fost niciodată simplă. Și pentru că atacurile evoluează în fiecare zi pe măsură ce atacatorii devin mai inventivi, este esențial să se definească în mod corespunzător ce este securitatea cibernetică și să se identifice bune practici și procese pentru o bună securitate cibernetică.

De ce este atât de important? Deoarece an de an, cheltuielile la nivel mondial pentru securitatea cibernetică continuă să crească. Organizațiile încep să înțeleagă că malware-ul este disponibil publicului, care face mai ușor pentru oricine să devină un atacator cibernetic și chiar și mai multe companii oferă soluții de securitate care nu fac nimic pentru a apăra împotriva atacurilor. Securitatea cibernetică necesită concentrare, evoluție continuă și dedicare.

Tehnologii pentru asigurarea securității cibernetică

Ce este asigurarea și securitatea informației?

Când vorbim despre tehnologii pentru asigurarea și securitatea informației, ne referim la acele tehnologii ce sunt capabile să ofere un grad înalt de protecție a cunoștințelor, informațiilor, datelor procesate într-un anumit context.

Acest domeniu este construit pe baza a două discipline principale:

- Asigurarea informației
 - se focusează să asigure integritatea, autenticitatea, confidențialitatea și non-repudierea informațiilor și a sistemelor.
 - măsurile luate în această direcție pot include acțiuni precum implementarea sistemelor de reacție, detecție și protecție a datelor în fața riscurilor cibernetică.
- Securitatea informației se focusează pe protecția datelor și a sistemelor informatice în fața accesului neautorizat, manipularea și perturbarea datelor astfel încât să asigure disponibilitatea, confidențialitatea și integritatea acelor date.

Ce sunt controalele de securitate cibernetică?

Controalele de securitate cibernetică sunt esențiale, deoarece hackerii inovează și dezvoltă în mod constant moduri mai inteligente de executare a atacurilor, atacuri ce sunt susținute de progresele tehnologice.

În acest timp, organizațiile trebuie să pună în aplicare cele mai bune metode de protecție pentru a-și consolida pozițiile de securitate. Acest proces presupune respectarea standardelor internaționale, diverselor reglementări și implementarea strategiilor de apărare în conformitate cu tipul de date sau sistemul informatic deținut.

Controalele de securitate cibernetică sunt contramăsurile pe care companiile le implementează pentru a detecta, preveni, reduce sau contracara riscurile de securitate. Acestea sunt măsurile pe care o întreprindere le implementează pentru a gestiona amenințările care vizează sistemele și rețelele de calculatoare.

Obiectivele controalelor de securitate cibernetică

Controalele de securitate nu sunt implementate în mod arbitrar, ci sunt determinate în funcție de rezultatele unui proces de gestionare a riscurilor unei organizații. Acest proces începe cu definirea strategiei generale de securitate IT, apoi următorul pas este identificarea obiectivelor ce se doresc a fi atinse, după ce aceste controale de securitate sunt efectuate.

Odată ce o organizație definește obiectivele de control, poate evalua riscul pentru unul sau mai multe sisteme informatice și selectează cele mai adecvate controale de securitate.

Metode de protecție folosite în controalele de securitate cibernetică

1. Inventarierea și controlul periodic
pentru hardware

4. Politici de utilizare a drepturilor
administrative/ privilegiate

1. Inventarierea și controlul periodic
pentru software

5. Setări securizate pentru hardware,
stații, rețele, servere

3. Implementarea unui proces de
management a vulnerabilităților

6. Monitorizarea și analiza
log-urilor de sistem

Clasificarea controalelor de securitate cibernetică

Controalele de securitate pot fi clasificate astfel:

A. După tip

A.1 Controlul Tehnic

Definiție

Controalele tehnice reprezintă controale de securitate ce sunt executate de sistemele computerizate și pot oferi protecție automată împotriva accesului neautorizat sau a utilizării necorespunzătoare. De asemenea pot facilita procesul de detecție a anomaliilor și pot susține cerințele de securitate pentru aplicațiile și datele existente într-o anumită organizație.

Exemple de controale tehnice

- Encipția datelor
- Implementarea unui sistem de protecție tip: Antivirus și Anti-Malware
- Firewalls
- Implementarea unui sistem de protecție tip: Securitatea informațiilor și gestionarea evenimentelor (SIEM)
- Sisteme de detectare a intruziunilor (IDS) și sisteme de prevenire a intruziunilor (IPS)

A.2 Controlul Administrativ

Definiție

Controalele administrative definesc factorii umani de securitate. Acest tip de control implică toate nivelurile de personal din cadrul unei organizații și determină ce utilizatori au acces, la ce resurse și ce informații, în urma unui set de reguli bine definit.

Exemple de controale administrative

- Programe de instruire în materie de securitate oferită de organizație pentru angajați;
- Politici de gestionare a parolelor;
- Planuri de răspuns la incidente (ce vor influența alte tipuri de controale);
- Controale de gestionare a personalului (recrutare, generare de cont, roluri și privilegii).

A.3 Controlul Operațional

Definiție

Controalele de securitate operațională sunt cele care completează securitatea unei organizații printr-un set de metodologii ce utilizează atât elemente fizice, cât și tehnice. Securitatea operațională, denumită și securitate procedurală, cuprinde crearea și aplicarea politicilor, procedurilor ce trebuie respectate în cadrul unui spațiu enterprise.

Exemple de controale operaționale

- Politică de securitate generală
- Politică de instruire privind conștientizarea securității
- Politica biroului curat
- Politică privind dispozitivele mobile
- Planul de continuitate a afacerii
- Politică de recuperare în caz de dezastru
- Procedura de răspuns la incidente
- Diferite standarde internaționale ce trebuie respectate în funcție de tehnologiile cu care o organizație operează

A.4 Controlul Fizic

Definiție

Describe orice lucru tangibil folosit pentru a preveni sau detecta accesul neautorizat la zone fizice sau sisteme active.

Exemple de controale fizice

Metodele de protecție implementate în urma acestui tip de control sunt:

- garduri, porți
- gărzi, ecusoane de securitate și carduri de acces
- controale de acces biometrice
- camere de supraveghere
- senzori de mișcare

B. După funcție

B.1 Preventiv

Controalele preventive includ mecanisme, instrumente sau practici de securitate care pot descuraja sau atenua acțiunile sau evenimentele nedorite.

Exemple de controale preventive

- Detectare / prevenire malware
Toate sistemele informatice ar trebui să aibă instalat un software care identifică și previne programele malware. Software-ul anti-malware ar trebui să fie actualizat, astfel încât să poată preveni cele mai recente versiuni de malware să pătrundă și să atace sistemele computerului
- Actualizarea sistemelor și a softurilor folosite se face în mod constant, astfel încât procesul de exploatare a atacatorilor să nu fie ușor executat
- Politică de acces a utilizatorilor și angajaților din cadrul unei companii
Drepturile de acces ar trebui stabilite pe baza informațiilor de care au nevoie utilizatorii sau angajații pentru a-și îndeplini sarcinile de muncă.
De exemplu, managerul contabil nu ar trebui să aibă aceleași niveluri de acces în sisteme ca directorul financiar.
- Controlul accesului la rețea
Modul în care sistemele accesează rețeaua trebuie controlat urmând un set foarte strict de reguli pentru a elimina accesul neautorizat al utilizatorilor / angajaților la resurse virtuale critice și resurse fizice.
- Programe de instruire a angajaților privind riscurile cibernetică.
Utilizatorii și angajații unei organizații ar trebui să fie conștienți de riscurile și amenințările prezentate împotriva sistemelor și informațiilor pe care le utilizează.

B.2 Controlul Compensator

Definiție

Controlul compensator, numit și control alternativ, este un mecanism care este pus în aplicare pentru a îndeplini cerința unei măsuri de securitate care este considerată prea dificilă sau impracticabilă de implementat în prezent.

Exemple de controale compensatoare

- Separarea atribuțiilor
În funcție de profilul de activitate a unei organizații, separarea atribuțiilor între angajați poate fi o metodă de protecție vitală deoarece diminuează riscurile de manifestare a unei poziții administrative, într-un mod ce nu este benefic pentru organizație și părțile adiacente acesteia.
De ex. într-o companie cu profil financiar, puterea autoritară a unui director financiar este împărțită în mai multe părți, în funcție de contextul și structura companiei în cauză, pentru a diminua riscul fraudelor și a transferurilor ilegale de bani.

- Gardieni și agenți de securitate, această metodă reprezintă de asemenea și un tip de control preventiv.

B.3 Controlul corectiv

Definiție

Controalele de securitate corective includ măsuri tehnice, fizice și administrative care sunt implementate pentru a restabili sistemele sau resursele la starea lor anterioară după un incident de securitate sau o activitate neautorizată.

Exemple de control corectiv

- actualizarea unui sistem
- izolarea unui virus
- terminarea unui proces sau repornirea unui sistem.

De exemplu, punerea în aplicare a unui plan de răspuns la incidente este un exemplu de control administrativ corectiv.

B.4 Controlul Detectiv

Definiție

Controlul detectiv descrie orice măsură de securitate luată sau soluție implementată pentru a detecta activitățile nedorite sau neautorizate, ce sunt în desfășurare sau după au avut loc.

Exemple de controale detective

Exemple fizice includ:

- alarme sau notificări de la senzori fizici (alarme de ușă, alarme de incendiu) care alertează gardieni, polițiști sau administratori de sistem.

Exemple de execuție tehnică a controalelor detective

- Honeypot-urile și IDS (Sistem de detectare a intruziunilor)

B.5 Controlul Descurajator

Definiție

Controalele de acest tip descurajează comportamentul potențialilor atacatori sau angajaților rău intenționați.

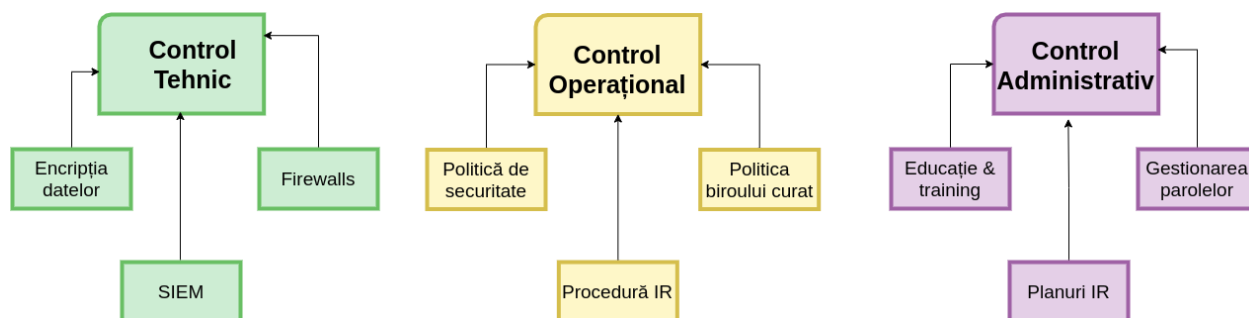
Exemple de controale descurajatoare

- Încuietorii ușilor
- Iluminatul
- camerele CCTV
- Semnalistică atenționare pentru diferite cazuri (ex Accesul interzis persoanelor neautorizate)
- suspensiile și amenziile sunt de asemenea controale de descurajare

Acestea sunt principiile de bază după care se construiesc ulterior politici de execuție a controalelor de securitate, iar pentru a obține un rezultat cât mai productiv, satisfăcător de pe

urma acestor politici, este nevoie ca sistemul de control ce este implementat într-o organizație, să fie mereu actualizat în conformitate cu ultimele tehnologii utilizate de companie și angajații acesteia.

Cele 3 tipuri principale de control de securitate cibernetică



Tehnologii pentru identificarea vulnerabilităților

Ce este o vulnerabilitate?

În contextul tehnologiei informației și securității cibernetice, o vulnerabilitate este un comportament sau un set de condiții prezente într-un sistem, produs, componentă sau serviciu care încalcă o politică de securitate implicită sau explicită. O vulnerabilitate poate fi considerată ca o slăbiciune sau expunere care manifestă un impact sau o consecință asupra securității.

Ce reprezintă un proces de identificare / detecție a vulnerabilităților?

Gestionarea vulnerabilităților este procesul de identificare, evaluare și raportare a riscurilor de securitate din sistemele informatice sau rețelele de calculatoare.

Categorii de procese de identificare a vulnerabilităților

- Evaluarea serverelor (hosts)
- Evaluarea rețelelor și a sistemelor wireless
- Evaluarea politicilor și practicilor pentru a preveni accesul neautorizat la rețelele private sau publice și la resursele accesibile rețelei.
- Evaluarea bazelor de date

- Scanări de aplicații - Identificarea vulnerabilităților de securitate în aplicațiile web și codul sursă al acestora prin scanări automate pe front-end sau analiza statică / dinamică a codului sursă.

Etapele unui proces de identificare a vulnerabilităților

Un proces de identificare a vulnerabilităților este construit pe baza a 4 pași principali:

1. Identificarea vulnerabilității sau a riscului (testare)

Analiștii de securitate testează starea de securitate a aplicațiilor, serverelor sau a altor sisteme scanându-le cu instrumente automate sau testându-le și evaluându-le manual. Scopul final acestui prim pas este de a construi o listă clară cu riscurile / vulnerabilitățile găsite pentru produsul / sistemul în testare.

2. Analiza vulnerabilității

Obiectivul acestui pas este de a identifica sursa și cauza principală a vulnerabilităților găsite în primul pas.

3. Evaluarea riscurilor

Obiectivul acestui pas este prioritizarea vulnerabilităților în funcție de riscul și impactul acestora asupra organizației afectate.

Procesul de evaluare trebuie însoțit și de un sistem de punctaj / scor ce să reflecteze tipul de vulnerabilitate găsit pentru un sistem dat vulnerabilitate:

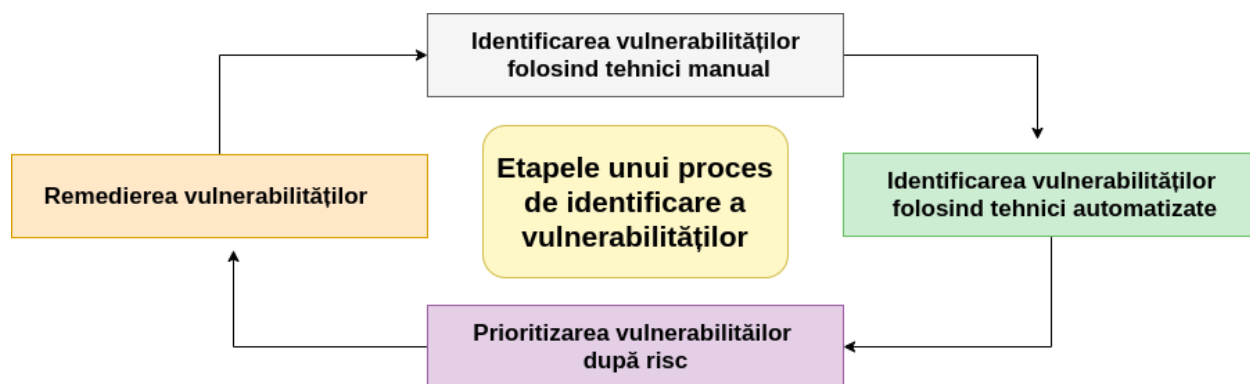
- Risc critic
- Risc înalt
- Risc mediu
- Risc minim
- Informațional

4. Remediere

Obiectivul acestui pas este fixarea problemelor de securitate. Este de obicei un efort comun al personalului de securitate, al echipelor de IT & Development, care determină calea cea mai eficientă pentru remedierea sau atenuarea fiecărei vulnerabilități.

Pașii specifici de remediere pot include:

- Introducerea de noi proceduri, măsuri sau instrumente de securitate.
- Actualizarea modificărilor operaționale sau de configurare.
- Dezvoltarea și implementarea unui patch de vulnerabilitate.



Tehnologii folosite în identificarea manuală și automată a vulnerabilităților

Arachni	Arachni	Gratuit	Majoritatea platformelor suportate
Burp Suite	PortSwigger	Gratuit / Comercial	Majoritatea platformelor suportate
Cyber Chief	Audacix	Comercial	SaaS sau On-Premise
Nessus	Tenable	Comercial	Windows
Netsparker	Netsparker	Comercial	Windows
Nikto	CIRT	Open Source	Unix/Linux

WPScan	WPScan Team	Comercial	Linux and Mac
Wapiti	Informática Gesfor	Open Source	Windows, Unix/Linux and Macintosh
Zed Attack Proxy	OWASP	Open Source	Windows, Unix/Linux, and Macintosh
w3af	w3af.org	Open Source	Linux and Mac

Tehnologii de anonimizare

Ce este un proces de anonimizare a datelor?

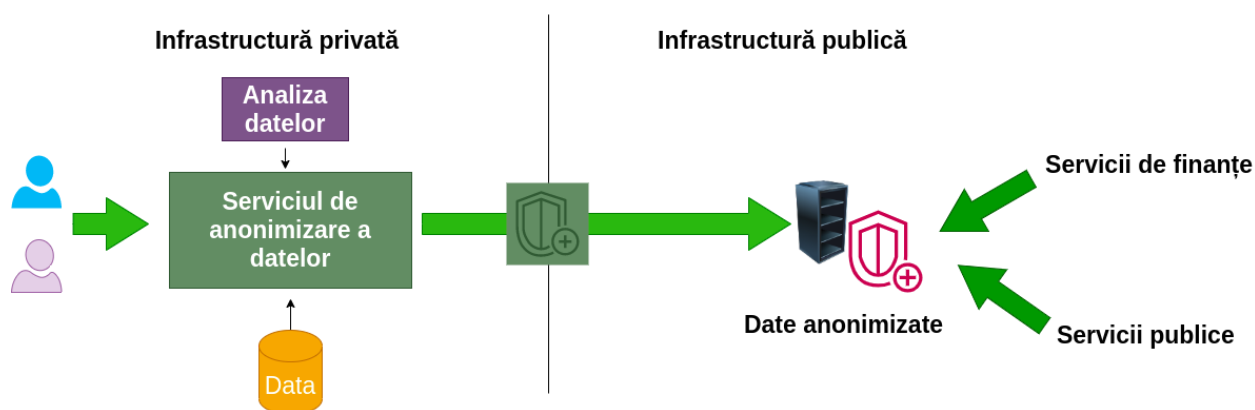
Anonimizarea datelor este procesul de protejare a informațiilor private sau sensibile prin ștergerea sau criptarea identificatorilor care conectează o persoană cu datele stocate.

Tehnici de anonimizare a datelor

- **Mascarea datelor** reprezintă procesul prin care valorile critice sunt ascunse cu valori modificate.
- **Pseudonimizarea** reprezintă procesul prin care se gestionează și se identifică datele a căror identificatori sunt înlocuiți cu pseudonime false.
Pseudonimizarea păstrează precizia statistică și integritatea datelor, permițând utilizarea datelor modificate pentru dezvoltare, testare și analiză, protejând în același timp confidențialitatea datelor.
- **Generalizarea datelor** reprezintă procesul prin care se elimină în mod deliberat unele date pentru a le face mai puțin identificabile.
Scopul este de a elimina unii dintre identificatori păstrând în același timp o măsură de acuratețe a datelor.
- **Schimbarea datelor** este procesul prin care se utilizează diferite tehnici de amestecare și permutare, cu scopul de a rearanja valorile atributelor setului de date, astfel încât acestea să nu corespundă cu înregistrările originale.
- **Date sintetice** este procesul prin care informațiile sunt fabricate algoritmic care nu au nicio legătură cu evenimente reale. Acest algoritm se bazează pe tiparele găsite în seturile de date originale.

Avantajele unui proces de anonimizare a datelor

1. Protejează împotriva breșelor de securitate
2. Oferă o garanție împotriva utilizării necorespunzătoare a datelor și a riscurilor de exploatare privilegiate
3. Oferă acreditarea companiilor de a utiliza datele utilizatorilor în fața diferitelor standarde internaționale precum: General Data Protection Regulation (GDPR) , Payment Card Industry Data Security Standard (PCI DSS) , Sarbanes–Oxley Act (SOX)



Tehnologii utilizate în procesul de anonimizare a datelor

ARX Data Anonymization Tool

- Program de tip Open Source ce permite anonimizarea datelor prin diferite tehnici, oferind utilizatorului și un GUI ce permite executarea procesului într-un mod facil.

Detalii:

<https://arx.deidentifier.org/>

Amnesia

- Avantajul acestui program este că oferă utilizatorului posibilitatea de a controla procesul de anonimizare, oferind un echilibru între confidențialitatea datelor și utilizarea acestora.

Detalii:

<https://amnesia.openaire.eu/>

u-Argus

- Acest instrument folosește o gamă largă de tehnici diferite de anonimizare, cum ar fi randomizarea, adăugarea zgomotului, micro agregarea datelor

Detalii:

<http://neon.vb.cbs.nl/casc/mu.html>

TOR

Tor este un software liber ce permite păstrarea anonimității pe internet printr-un algoritm de rutare din aproape-în-aproape. În rețeaua Tor, traficul online generat este anonim, fără a se înregistra lista de termeni căutați și fără a ține o evidență a IP-urilor de unde au fost inițializate respectivele căutări. Tor este recunoscut și ca poarta de intrare pentru așa zisele “Darknet” sau “Dark markets” sau “Internetul ascuns”.

<https://www.torproject.org/>

Atacuri și tehnici de inginerie socială

Ce sunt atacurile și tehnicile de inginerie socială?

Inginerie socială este termenul folosit pentru a însuma toate activitățile malițioase realizate prin interacțiuni umane.

Tehnicile de inginerie socială sunt construite pe baza metodelor de manipulare psihologică și aplicate de atacatori sau angajați rău intenționați cu scopul de a obține acces neautorizat, date critice sau de a executa transferuri ilicite de bani.

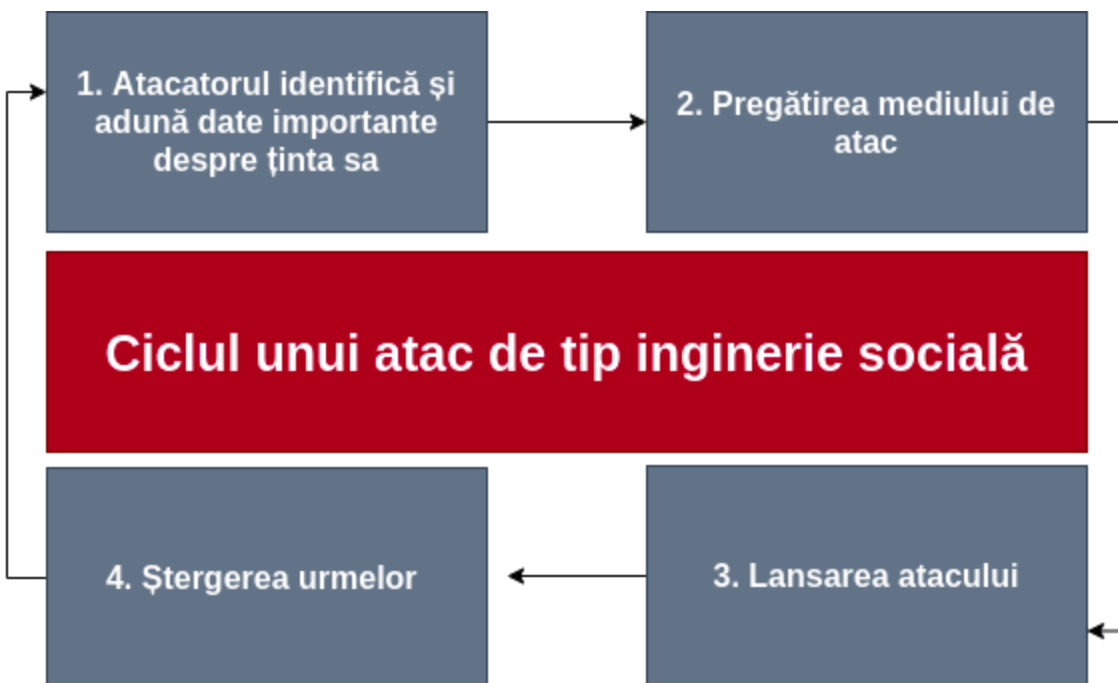
Care sunt pașii unui atac de inginerie socială?

Atacurile de inginerie socială au loc în mai mulți pași, drept urmare putem enumera:

- Primul pas pentru un atacator este să obțină informațiile necesare pentru a iniția și obține ulterior încrederea victimei.
- Lansarea atacului
- Ștergerea urmelor

Ceea ce face ingineria socială deosebit de periculoasă este că se bazează pe erori umane, mai degrabă decât pe vulnerabilități în software și sisteme de operare. Greșelile făcute de utilizatorii legitimi sunt mult mai puțin previzibile, ceea ce le face mai greu de identificat și contracarat decât o intruziune bazată pe malware sau alte metode de atacuri cibernetice.

Tehnici de atacuri de inginerie socială



Baiting

Atacurile de tip baiting folosesc o promisiune falsă pentru a stârni lăcomia sau curiozitatea victimei. Această tehnică are ca scop atragerea utilizatorilor într-o capcană care le fură informațiile personale sau le infectează sisteme operaționale cu malware.

Exemple

- O persoană rău intenționată plasează strategic un USB infectat cu malware, de ex în fața unei companii IT , spațiu în care unul sau mai mulți angajați ar fi curioși să conecteze acel USB găsit întâmplător în unul din calculatoarele companiei.
- Oferte de tip reclamă virtuală cu ajutorul cărora utilizatorii-victimă sunt atrași spre a accesa respectivele promoții, scopul atacului fiind exfiltrarea datelor personale, financiare (datele de pe cardul de cumpărături)

Scareware

Acest tip de atac implică bombardarea victimelor cu alarme false și amenințări fictive. Utilizatorii sunt înșelați să creadă că sistemul lor este infectat cu programe malware, determinându-i să instaleze software care nu are niciun beneficiu real, software ce reprezintă un malware în sine.

Un exemplu obișnuit de scareware îl reprezintă bannerele pop-up cu aspect legitim care apar în browser . în timp ce se navighează pe web, afișând texte precum:

Computerul dvs. poate fi infectat cu programe spyware dăunătoare!

Scareware este, de asemenea, distribuit și prin e-mail spam

Pretexting

Acest atac implică obținerea informațiilor printr-o serie de minciuni inteligente.

Un bun exemplu în acest caz ar fi când un faptuitor pretinde că are nevoie de informații sensibile de la o potențială victimă cu scopul de a îndeplini o sarcină critică (transfer urgent de bani, schimbarea parolelor într-un timp foarte limitat, etc)

Un factor vital în executarea cu succes a acestui tip de atac este obținerea încrederii victimei, care practic ulterior este transformată în ‘instrumentul atacului’, drept urmare atacatorii pot petrece chiar luni, ani în mod strategic pentru tatonarea terenului, obținerea de informații critice, astfel încât rata succesului să fie cât mai ridicată.

Phishing

Acest tip de atac este unul dintre cele mai populare tehnici de inginerie socială, ce reprezintă un mare risc pentru companiile mici și mari, drept urmare instruirea angajaților în această direcție este un pas vital.

Atacurile de tip phishing sunt de obicei campanii malițioase ce sunt distribuite prin intermediul serviciilor de email, iar un exemplu ar fi următorul scenariu:

1. Maria lucrează în cadrul unei companii cu profil IT, dar la departamentul de Resurse Umane.
2. Intr-o zi, Maria primește un email în care i se transmite următorul mesaj:
“Contul tău urmează să fie dezactivat în următoarele 10 min, în urma unor politici interioare ce au fost implementate astăzi. Pentru a evita acest lucru, te rog accesează link-ul de mai jos și resetează-ți parola.

Semnat,
Departamentul I.T Management”

3. Maria fiind constrânsă de urgență mesajului și autoritatea semnăturii, accesează link-ul oferit unde își introduce date contului, așa cum scrie în instrucțiunile primite pe email
4. Astfel atacatorul obține credențialele de autentificare a potențialelor victime sau accesul la resurse și seturi de date ce au acces limitat către public.

Spear phishing

Acest tip de atac este foarte asemănător ca și execuție cu tehnicile de atac de tip phishing, diferența dintre ele este că spear phishing presupune un pas additional și anume obținerea de informații despre potențială victimă, ce poate fi un sistem, persoana fizică, companie, etc, folosind tehnologii și instrumente precum: OSINT, Shodan, Frida, etc.

Metode de prevenire a atacurilor de inginerie socială

Inginerii socială manipulează sentimentele umane, cum ar fi curiozitatea sau frica, pentru a realiza scheme de atac și a atrage victimele în capcanele lor, prin urmare, fiți atenți ori de câte ori vă simțiți alarmat de un e-mail, atras de o ofertă afișată pe un site web, etc.

Următoarele recomandări ne ajută să ne accentuăm vigilența în legătură cu atacurile și tehnicile de inginerie socială:

- Nu deschideți e-mailuri și atașamente din surse suspecte
 - Dacă expeditorul este necunoscut, nu trebuie să răspundem la respectivul e-mail.
 - În cazurile în care expeditorul este totuși cunoscut, dar mesajul primit trezește suspiciuni, este recomandat ca acea informație primită să fie verificată și din alte surse: apel telefonic expeditor, mesaj scris, comunicare prin platforme sociale.
- Utilizați autentificarea multifactorială - Una dintre cele mai valoroase informații pe care le caută atacatorii sunt credențialele utilizatorului.
- Atenție la ofertele ispititoare primite prin surse precum: email, apel telefonic, reclama pe site-uri web, mesaje text de tip SMS, mesaje private de pe platformele sociale, etc.
- Software-ul antivirus / antimalware trebuie actualizat periodic în conformitate cu ultimele tipuri de atacuri, astfel încât procesul de detecție să fie cât mai productiv.

Managementul parolelor și tehnici de spargere parolelor

Ce este managementul parolelor?

Deși parolele rămân în continuare una dintre cele mai sigure metode de autentificare disponibile până în prezent, acestea sunt supuse unui număr de amenințări la adresa securității atunci când sunt tratate greșit, iar aici intervine rolul de gestionare a parolelor, ce are ca scop protejarea datelor de autentificare a utilizatorilor prin diferite metodologii de encriptie, stocare, etc.

Ce provocări sunt întâlnite în gestionarea parolelor?

Când numărul serviciilor web utilizate de persoane fizice, dar și de companii, crește de la un an la altul, numărul infracțiunilor cibernetice de asemenea crește.

Iată câteva exemple ce reprezintă reale riscuri ce vizează felul în care un utilizator își configurează parolele, codurile de acces pentru diferite servicii folosite.

Login spoofing

Parolele sunt colectate ilegal printr-o pagină falsă de autentificare de către infractorii cibernetici.

Atac de tip sniffing

Parolele sunt furate folosind accesul ilegal la rețea și cu instrumente cum ar fi Keyloggers, Rootkits, backdoors, atacuri de tip man-in-the-middle.

Shoulder surfing attack

Este o metodă de atac ce presupune ca atacatorul să folosească diferite instrumente precum microcamerele, astfel încât să poată înregistra datele de autentificare a unei victime sau încercă să privească indiscret astfel încât să poată obține o perspectivă asupra metodelor de autentificare folosite de victimă.

Brute-force attack

Este o metodă de atac prin care atacatorul lansează instrumente automatizate, cu scopul de a obține baze de date ce conțin credențialele utilizatorilor, coduri de autentificare, parole, etc.

Ce metode de protecție putem folosi împotriva acestor atacuri?

- Utilizați parole complexe și unice pentru toate site-urile, serviciile și aplicațiile puternice.
- Resetați parolele la intervale regulate de timp.
- Configurați autentificarea folosind metode precum 2FA sau MFA (multi-factor-authentication).
- Stocați toate parolele companiei și cele personale, într-un singur loc folosind programe precum Bitwarden, Keepass, etc.

Participarea la programe de tip bug bounty

Ce este un program de tip bug bounty?

Programele de tip bounty reprezintă un set de oferte oferite de multe site-uri web, organizații și dezvoltatori de software prin care persoanele participante pot primi recunoaștere și câștiguri financiare pentru raportarea erorilor, în special a celor referitoare la exploatarea și vulnerabilitățile de securitate cibernetică.

Raportările sunt realizate de obicei printr-un program condus de un third-party (cum ar fi Bugcrowd sau HackerOne), ce pune la dispoziție un program și un mediu de testare, adaptat după pentru nevoile organizației.

Cine apelează la programele de tip bug bounty?

Multe organizații importante folosesc programe de tip bug bounty, ca o măsură adițională a politicilor de securitate implementate. Printre aceste organizații, putem numi: Android, Apple, Digital Ocean, Amazon, eBay, PayPal, ec..

O listă cu programele bug bounty actuale, oferite de HackerOne și BugCrowd pot fi vizualizate accesând link-urile de mai jos:

<https://www.bugcrowd.com/bug-bounty-list/>

<https://www.hackerone.com/>

De ce companiile optează pentru programele de tip bounty?

Programele de tip bug bounty oferă organizațiilor disponibilitatea de a lucra cu mai mulți specialiști de securitate cibernetică, aspect ce permite identificarea vulnerabilităților într-o perioadă scurtă de timp, oferind o perspectivă rapidă clientului asupra măsurilor de securitate ce trebuiesc implementate în cadrul companiei sale.

De ce participă cercetătorii și specialiștii în domeniu la programele bug bounty?

Găsirea și raportarea erorilor printr-un program de tip bug bounty poate aduce atât bonusuri financiare, dar și la recunoaștere. Cei mai buni hackeri ce participă în genul acesta de programe ajung să fie invitați să audieze produse selecte în programe private, din diferite industrii, oferindu-le posibilități de câștig semnificativ mai mari față de celelalte programe de acest gen de pe o platforma data. În medie, pentru fiecare vulnerabilitate un specialist poate primi sume începând cu 500\$ și ajungând la \$100,000 sau depășind în cazuri excepționale.

De asemenea, în unele cazuri poate fi o modalitate excelentă de a căpăta experiență și a aprofunda cunoștințele tehnice dobândite, aspecte ce pot reprezenta reale avantaje atunci când apare posibilitatea unui interviu în cadrul unei organizații.

Pe lângă avantajele prezentate mai sus, participarea la astfel de programe poate fi și distractivă! Este o șansă mare și legală de a vă testa abilitățile împotriva tehnologiilor și a sistemelor de protecție implementate de companii mari, medii și mici.

Platforme ce oferă programe de tip bug bounty

- BugCrowd
- HackerOne
- Intigriti

- YesWeHack

Dezvoltarea unui business sau startup în securitate cibernetică

Ce este un Startup?

Startup-ul este o companie, un parteneriat sau o organizație temporară care există pentru a căuta un model de afaceri replicabil și scalabil. O caracteristică importantă ce diferențiază startup-ul de o companie la început de drum este potențialul de creștere exponențială, motiv pentru care, în general, atunci când auzim termenul de startup ne gândim la o companie care dezvoltă tehnologie.

Startup-urile și companiile consacrate oferă clienților produse sau servicii. **Produsul** este un bun pentru care clientul plătește o dată, după care îl deține, de ex. un calculator, un obiect de îmbrăcăminte, o licență permanentă pentru un antivirus. **Serviciul** este un beneficiu pe care clientul îl primește pe perioada pentru care plătește pentru el, de ex. abonamentul de telefonie și internet, închirierea unui apartament, accesul la o sală de fitness.

O sintagmă des întâlnită este SaaS (software as a service), ce e practic transformarea licențelor permanente software din trecut, în accesul temporar la un program, pe baza unui abonament – ex. abonament lunar la un antivirus, ce primește update-uri dese, însă accesul se pierde imediat ce clientul încetează plata abonamentului.

Care sunt etapele de dezvoltare prin care trece un startup?

De la idee până la etapa de final a unui startup, fondatorii vor trece prin câteva momente cheie în dezvoltarea companiei. Unele dintre următoarele etape vor fi parcurse în paralel, în funcție de specificul echipei, a strategiei de creștere alese și a pieței adresate.

Găsirea ideii

Identificarea ideii pe baza căreia fondatorul pornește startup-ul poate fi un proces spontan sau intenționat. Sunt cazuri de fondatori care observă – la ei sau la oamenii din jur – nevoi neadresate sau deservite de produse nesatisfăcătoare. De asemenea, sunt experți tehnici care învață noi tehnologii și descoperă potențiale utilizări valoroase ale acestor tehnologii. Astfel, pe baza unor observații proprii, fondatorii pornesc în dezvoltarea unor produse inovatoare.

Există de asemenea antreprenori sau echipe care își propun să creeze un startup și parcurg un proces intenționat de identificare de oportunități. În general, în aceste cazuri e vorba de echipe de oameni ce provin din domenii diferite (precum agricultură, sănătate, arhitectură etc) ce

combină cunoașterea unei industrii cu înțelegerea tehnică necesară dezvoltării de produse inovatoare ce deservește nevoile identificate. Fondatorii caută diverse idei, pe care ulterior le verifică cu diverși oameni din industria vizată.

Citește mai mult: [Design Thinking](#)

Formarea echipei

De multe ori echipa de bază se formează concomitent cu găsirea ideii. Este foarte important pentru dezvoltarea de succes a startup-ului ca echipa de fondatori să aibă expertiză diversă – cunoștințe de programare și dezvoltare de tehnologie, cunoștințe de business și marketing, skill-uri de comunicare și relaționare cu clienții și utilizatorii.

La fel de importantă este experiența de lucru împreună a fondatorilor și încrederea reciprocă ce îi va ajuta pe membrii fondatori să parcurgă etapele frumoase, dar și grele, care vor apărea în mod sigur pe măsură ce vor dezvolta produsul și compania.

În mod excepțional există startup-uri dezvoltate de un singur fondator, ce acoperă o plajă mare de expertiză și este foarte determinat să reușească. În general, investitorii și mentorii startup-urilor încurajează crearea echipelor cât mai devreme, pentru a beneficia de perspective diferite, putere mai mare de execuție în timp scurt și back-up pentru situații neprevăzute.

Testarea pieței

Ideea de bază și prima schiță a produsului vor fi dezvoltate de echipa de fondatori. Este foarte important ca acestea să fie schițate cu o categorie de utilizatori anume în minte, pentru a analiza nevoi și probleme concrete ce trebuie rezolvate.

Piața este reprezentată de persoanele individuale sau companiile ce pot cumpăra produsul sau serviciul dezvoltat de către startup.

Problema adresată și modalitatea de implementare trebuie validate cât mai devreme, cu entități cât mai diverse din piața țintă. Validarea se poate realiza prin dezvoltarea unui prototip și cererea de feedback pe baza acestuia sau, chiar înainte, prin sondaje și conversații despre experiența actuală și eventualele neajunsuri resimțite de oamenii adresați (cercetare cantitativă și calitativă a pieței).

Citește mai mult: [Customer Development](#)

Crearea unui prototip

Primul pas în dezvoltarea produsului este crearea unui prototip ce demonstrează că problema adresată poate fi rezolvată. În cazul produselor ce aduc tehnologii inovative, primul pas foarte important este demonstrarea că inovația propusă poate fi implementată.

Dacă este vorba de produse ce nu prezintă provocări tehnologice majore, care în general aduc inovări în modelul de business sau adresează probleme încă nerezolvate, prototipul validat inițial cu clienții poate fi chiar și o interfață desenată, un wireframe sau un flux de lucru schematizat. Important este să poată fi explicat potențialilor clienți, cu scopul de a valida primii pași.

O sintagmă des întâlnită e conceptul de MVP (Minimum Viable Product), ce descrie setul minimal de feature-uri pe care clientul le poate utiliza pentru a-și deservi nevoia și a oferi feedback pentru dezvoltarea ulterioară a produsului.

Dezvoltarea modelului de business

Modelul de business este planul prin care compania creează, livrează și capturează valoare. Construind și iterând pe modelul de business, antreprenorii fac vizibile următoarele elemente vitale ale companiei:

Element de business	Exemplu
Valoarea livrată clienților	Protecție împotriva virusilor
Segmente de utilizatori adresate	Persoane individuale, companii ce își protejează angajații
Canale de distribuție	Website propriu, platforme de vânzări software
Interacțiuni cu clienții	Vânzări, suport tehnic
Activități cheie	Dezvoltare software, cercetare antivirus, promovare
Resurse cheie	Experți tehnici, resurse de hosting, platforme de programare
Parteneri	Platforme de revânzare software, site-uri de promovare antivirusi
Surse de venit	Vânzarea licențelor lunare
Structura costurilor	Salarii angajați, abonament hosting, licențe software de programare, reclame online

Toate elementele de mai sus trebuie definite și actualizate în timp astfel încât raportul venituri / cheltuieli să fie cât mai mare. Unele startup-uri atrag finanțări externe, ceea ce le permite să

mențină un timp un raport venituri / costuri negativ, pentru a dezvolta tehnologia și a crește rapid numărul de utilizatori. Momentul în care raportul devine zero se numește break-even, iar apoi compania devine profitabilă.

Citește mai mult: [Business Model Canvas](#)

Dezvoltarea strategiei de marketing

Strategia de marketing descrie modalitatea prin care startup-ul își propune pe termen lung să-și dezvolte în mod sustenabil avantajul competitiv, prin înțelegerea și deservirea nevoilor clienților.

Pentru a defini strategia de marketing, se pornește de la obiectivele de business (ex. încasări dorite într-o perioadă de jumătate de an), ținând cont de nevoile și preferințele utilizatorilor, se dezvoltă un plan de acțiuni de promovare ce vor susține eforturile de vânzări, ținând cont de bugetul ce poate investi pentru promovare.

Activități de promovare pot fi:

- reclame pe Facebook, Google, YouTube etc.
- review-uri plătite pe bloguri sau în podcasturi
- oferirea produselor proprii ca și premii în diverse concursuri
- afișaj de mari dimensiuni în orașe
- prezența cu stand-uri de testare în evenimente
- recompensarea utilizatorilor pentru aducerea în aplicație de noi utilizatori

Atragerea unor finanțări

Pentru a putea testa mai rapid ipotezele de produs și business, pentru a crește mai rapid și a putea dezvolta o echipă valoroasă mai repede, startup-urile pot alege să atragă finanțări externe.

Prin oferirea unei finanțări, o persoană sau o companie externă oferă o sumă de bani startup-ului în schimbul unui procent din acțiunile firmei, cu speranța că în viitor își va recupera investiția și va face profit (prin vânzarea acțiunilor deținute sau prin obținerea de dividende).

Startup-urile pot primi finanțări de la:

- **Angel investors** – investitori individuali care investesc din averea proprie; în general se implică în companii din domenii de expertiză pe care le stăpânesc, oferă capital la începutul afacerii și aduc beneficii importante de mentorat pentru antreprenori
- **Acceleratoare de business** – programe care aduc o investiție de început, cuplată cu un program educațional pentru antreprenori și deschidere către potențiali clienți
- **Fonduri de venture capital (VCs)** – fonduri care investesc sume mari de bani, în general în startup-uri care au clienți plători și un model de business scalabil deja dovedit

- **Granturi de cercetare** – sunt oferite de organisme naționale sau internaționale care susțin inovarea și cercetarea și în general sunt sume de bani ce nu presupun cedarea de acțiuni în firmă, ci dovedirea parcurgerii unor etape de dezvoltare.

Sunt startup-uri și companii care aleg să nu atragă finanțări externe, care cresc doar prin eforturile echipei și prin reinvestirea profitului în dezvoltarea companiei. Modalitatea aceasta de creștere se numește boot-strapping (companii care “se trag singure de șireturi în sus”).

Scalarea

După ce un startup ajunge la momentul de product-market fit (dovedește că dezvoltă un produs valoros, ce este cumpărat de o categorie destul de mare de oameni sau companii astfel încât compania să poată fi profitabilă) este momentul ca echipa să se concentreze pe scalarea afacerii.

Prin activități de marketing și de vânzări, startup-ul își propune să ajungă la cât mai mulți potențiali clienți și să-și vândă produsul sau serviciul. Echipa și activitățile pe care le desfășoară trebuie crescute în mod proporțional cu nevoile clienților deserviți.

În cazul startup-urilor ce reușesc să scaleze exponențial, nevoia de a crește echipa și cheltuielile operaționale crește mult mai lent decât încasările obținute de la clienți. De exemplu, un produs software care își crește exponențial numărul de clienți trebuie să crească treptat capacitatea de a răspunde la cererile de suport și cheltuielile de hosting în timp ce veniturile cresc mult mai rapid. O companie care oferă servicii de curățenie în schimb, pentru a deservi mai mulți clienți, trebuie să angajeze proporțional mai mulți angajați, deci își va crește profitul liniar, niciodată exponențial (fără elemente de automatizare).

Strategia de exit

În funcție de strategia adoptată, succesul startup-ului pe termen lung poate lua mai multe forme:

- transformarea într-o companie sustenabilă, cu un model de business bine definit, ce poate alternativ să aleagă să-și diversifice oferta de produse sau servicii și să continue pe termen lung ca o companie independentă, la nivel național sau multi-național; va returna eventualele investiții de parcurs prin dividende (părți proporționale din profitul anual)
- vânzarea către un jucător mai mare din piață, care poate fi interesat de tehnologie, baza de clienți și/sau echipă; va returna profit către eventualii investitori și fondatori prin răscumpărarea acțiunilor deținute la o valoare mai mare decât cea inițială
- listarea pe bursă (IPO), prin care compania listează o parte din acțiunile firmei către public, ceea ce permite oricăror acționari anteriori să-și vândă acțiunile deținute la momentul pe care fiecare îl consideră optim, în funcție de valoarea zilnică pe bursă a companiei; la nivel operațional, se aseamănă cu prima variantă, compania dezvoltându-se și diversificând în timp oferta

Startup-uri românești de securitate

Ecosistemul românesc de startup-uri este în plină expansiune. Antreprenorii au o multitudine de oportunități de învățare, finanțare locală și internațională, atenția presei și disponibilitatea de colaborare din partea companiilor mari și multi-naționale.

Iată câteva startup-uri românești care s-au remarcat în ultimii ani în domeniul securității cibernetice. O parte din ele continuă să se dezvolte prin forțe proprii, cu ajutorul partenerilor sau investitorilor, unele au ajuns să fie achiziționate de către companii mari internaționale aflate în expansiune și unele, precum TypingDNA, și-au mutat sediul principal în SUA, pentru a fi mai aproape de investitorii și clienții principali, păstrând în continuare parte din echipa tehnică în România.

Pentest Tools

Fondat în 2013 de Adrian Furtună, Pentest-Tools.com este un serviciu online care permite utilizatorilor să testeze securitatea site-urilor și a infrastructurii de rețea expuse la internet. Serviciul oferă o colecție de instrumente specializate de testare a securității care pot fi utilizate de proprietarii site-urilor web, de administratori de rețea și sisteme și de experți pentru a-și face propriile evaluări de securitate.

Scopul Pentest-Tools.com este de a simplifica procesul de testare a securității prin oferirea unei interfețe [web](#) ușoare pentru instrumente complexe, rapoarte detaliate cu vulnerabilități și recomandări pentru îmbunătățirea securității.

Citește mai mult:

- [Pentest Tools – primul startup românesc prezent la Black Hat Europe](#)
- [După mulți ani în care a fost ethical hacker într-o multinațională, și-a lansat propriul proiect: Startup-ul ce verifică siguranța site-urilor](#)

Dekeneas

Fondat în 2017 de Andrei Bozeanu, Dekeneas e un startup care se adresează companiilor de mari dimensiuni sau instituțiilor publice care au provocări în momentul trecerii în online cu protecția în fața posibilelor atacuri.

Dekeneas folosește inteligența artificială și machine learning ca să detecteze atacuri complexe, cum ar fi cele de tip „watering hole” (infectarea unui [site](#) popular, vizitat de un număr mare de persoane) sau cryptojacking (injectarea de software malițios care folosește calculatoarele vizitatorilor unui site pentru minarea de monedă virtuală).

Citește mai mult:

- [ZF IT Generation ZF IT Generation. Andrei Bozeanu, fondator Dekeneas, o platformă de detecție a atacurilor cibernetice](#)
- <https://start-up.ro/startup-ul-local-dekeneas-300-crestere-si-oferte-de-un-milion-de-euro-refuzate>

Appsulate

Fondat în 2016 de către Alex Negrea (România) și Uli Mittermaier (SUA), cu echipa de dezvoltare tehnică în București, Appsulate a dezvoltat o platformă ce permitea accesul în aplicații ce conțineau date sensibile printr-un mediu protejat împotriva atacurilor de tip malware, împiedicând, totodată, pierderea sau furtul datelor.

În 2019 Appsulate a fost cumpărat de către Zscaler, furnizor global de servicii de securitate cibernetică, cu sediul în San Jose, California, fondat în 2011 și listată pe NASDAQ din luna martie 2018, cu are o valoare de piață evaluată la 10 miliarde de dolari la momentul în care a achiziționat Appsulate.

Citește mai mult:

- [Startup-ul Appsulate, cu fondator român, cumpărat de unicornul Zscaler](#)

TypingDNA

Fondat în 2016 de către Raul Popa și Cristian Tămaș, TypingDNA oferă soluții suplimentare de securitate folosindu-se de amprenta biometrică a tastatului.

TypingDNA a dezvoltat algoritmi și tehnologii proprii de inteligență artificială pentru autentificarea utilizatorilor în funcție de modul în care aceștia utilizează tastatura. Printr-un proces de observare și învățare a modului în care utilizatorul tastează, TypingDNA poate recunoaște încercările ulterioare ale unui anumit utilizator prin potrivirea lor cu contul cunoscut.

Din 2020 compania și-a mutat sediul principal în New York, a absolvit programul global Techstars și a atras până acum finanțări totale (în mai multe runde de investiții) de peste 8,8 milioane de dolari.

Citește mai mult:

- [Românii de la TypingDNA au obținut o finanțare de 7 de milioane de dolari. Fac angajări și în România](#)
- [5 Questions with Raul Popa \(TypingDNA\): Adding a security blanket to the Internet](#)

- [#BeAI - Typing Biometrics. TypingDNA: hindsight CEO view with Raul Popa](#)

Bit Sentinel

Fondat în 2015 de către Andrei Avădănei, Bit Sentinel este una dintre cele mai importante companii românești ce furnizează servicii de securitate cibernetică, sprijinind organizații din domenii diverse precum sănătate, comunicații, retail, transport, financiar-bancar și prin servicii de consultanță și audit de securitate, penetration testing, servicii de monitorizare și răspuns la incidente.

Compania este implicată activ în numeroase inițiative de stimulare a industriei locale de securitate cibernetică, fiind și unul din antrenorii echipei naționale pentru Campionatul European de Securitate Cibernetică, încă din 2018, câștigând alături de lotul național al României ediția din 2019. Bit Sentinel este și unul din inițiatorii UNbreakable România.

Citește mai mult:

- [Românii de la Bit Sentinel vor fi coordonatorii tehnici ai Campionatului European de Securitate Cibernetică de la București](#)
- [Bit Sentinel extinde portofoliul de servicii și echipa. „Trăim într-o lume în care este o chestiune de timp până când un atac cibernetic are loc.”](#)
- [Bit Sentinel promite scurtarea timpului de răspuns la incidente cibernetice cu ajutorul unei noi divizii CERT](#)

CyberEDU

Fondat în 2020 ca un spin-off BIT SENTINEL, [CyberEDU](#) a fost creat inițial ca o platformă în care orice utilizator poate rezolva exerciții din concursuri de cybersecurity în ritmul său. În scurt timp, platforma a iterat, devenind platforma educațională necesară pentru a încuraja și facilita educația în securitate cibernetică. În 2020 CyberEDU a fost acceptat în Programul European IMPACT EdTech (din peste 300 de alte startup-uri europene) pentru etapa de incubare și mai apoi a fost selectată și pentru etapa de accelerare. Orice organizație din mediul academic sau privat poate folosi CyberEDU ca un instrument puternic de e-learning pentru cei care doresc să învețe cunoștințe practice de securitate cibernetică. Soluția pune la dispoziție funcționalitățile necesare pentru organizarea de exerciții practice și laboratoare red sau blue team și competiții de cyber security, platforma având și o bază de date cu peste 200 de exerciții practice și suport teoretic, aliniat la standarde internaționale precum OWASP, MITRE sau CWE pentru a susține activitatea trainerilor, profesorilor și a utilizatorilor.

Mai mult decât atât, platforma CyberEDU găzduiește și o serie de competiții importante de securitate cibernetică dintre care amintim: DefCamp Capture the Flag și Romanian Cyber Security Challenge.

Citește mai mult:

- [CyberEDU a fost printre cele 7 startup-uri selectate de a merge în etapa de accelerare la IMPACT EdTech](#)
- [Romanian Cyber Security Challenge – RoCSC a avut loc pe platforma educatională CyberEDU](#)

Resurse utile pentru antreprenori

- Steve Blank – The startup owner's manual - <https://steveblank.com/>
- Paul Graham – Essay: Startup equals growth - <http://www.paulgraham.com/growth.html>
- Rob Fitzpatrick - The Mom Test - <https://robfitz.com/>
- Startup School by YCombinator – program gratuit online pentru antreprenori - <https://www.startupschool.org/>

Pregătire pentru UNbreakable România

Care sunt regulile și limitările generale pentru participanți?

- La competiția individuală nu ai voie să colaborezi, iar la competiția pe echipe 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 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, întrebări moderatorii pe canalul de discord sau prin email.
- Dacă este prima data cand participi la un astfel de concurs, ar trebui sa stii ca o soluție (flag) este un cod pe care ar trebui sa il identifici atunci când rezolvi un task. Nu exista o procedura standard pentru a le găsi, este recomandat sa faci mai multe teste și sa nu-ti limitezi gandirea pentru a le obține. În cele din urma, veti înțelege dinamica acestui tip de concurs CTF si cum sa rezolvati rapid provocarile.
- Dacă sunteți sigur ca ați identificat soluția corectă (flag-ul este 100% corect) dar sistemul nostru nu acceptă să-l transmiteți, informați-ne prin chat, in privat fara sa divulgați flag-ul
- Dacă identificați și ne raportați erori în infrastructură de concurs, puteți fi recompensați
- Avem un clasament dinamic, ceea ce înseamnă ca cu cat mai multe echipe rezolva o provocare, cu atat punctajul problemei scade.
- 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 intrebari comune si regulament: <https://unbreakable.ro/regulament>

Care sunt și cum se calculează criteriile de evaluare?

Principalul obiectiv al UNbreakable Romania este de a încuraja tinerii să participe la competiții de securitate cibernetică. Un alt obiectiv important este crearea unui mecanism de evaluare pentru aceștia. Fiecare sezon are mai multe etape de concurs. Fiecare etapă de concurs (eg. etapa individuală, etapa pe echipe) are un clasament dedicat. Fiecare etapă are mai multe exerciții. Lipsa participării la o etapă nu afectează rezultatele altei etape, dar clasamentul final pe sezon poate fi influențat.

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 jucător ce a obținut puncte va fi încadrat în una din categoriile următoare în fiecare etapă:

- Gold - Top 15% jucători individuali sau echipe
- Silver - Top 15-35% jucători individuali sau pe echipe
- Bronze - Top 35-50% jucători individuali sau pe echipe

Punctajul unui exercițiu

Modalitatea de calcul pentru punctele primite alocate fiecărui exercițiu 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

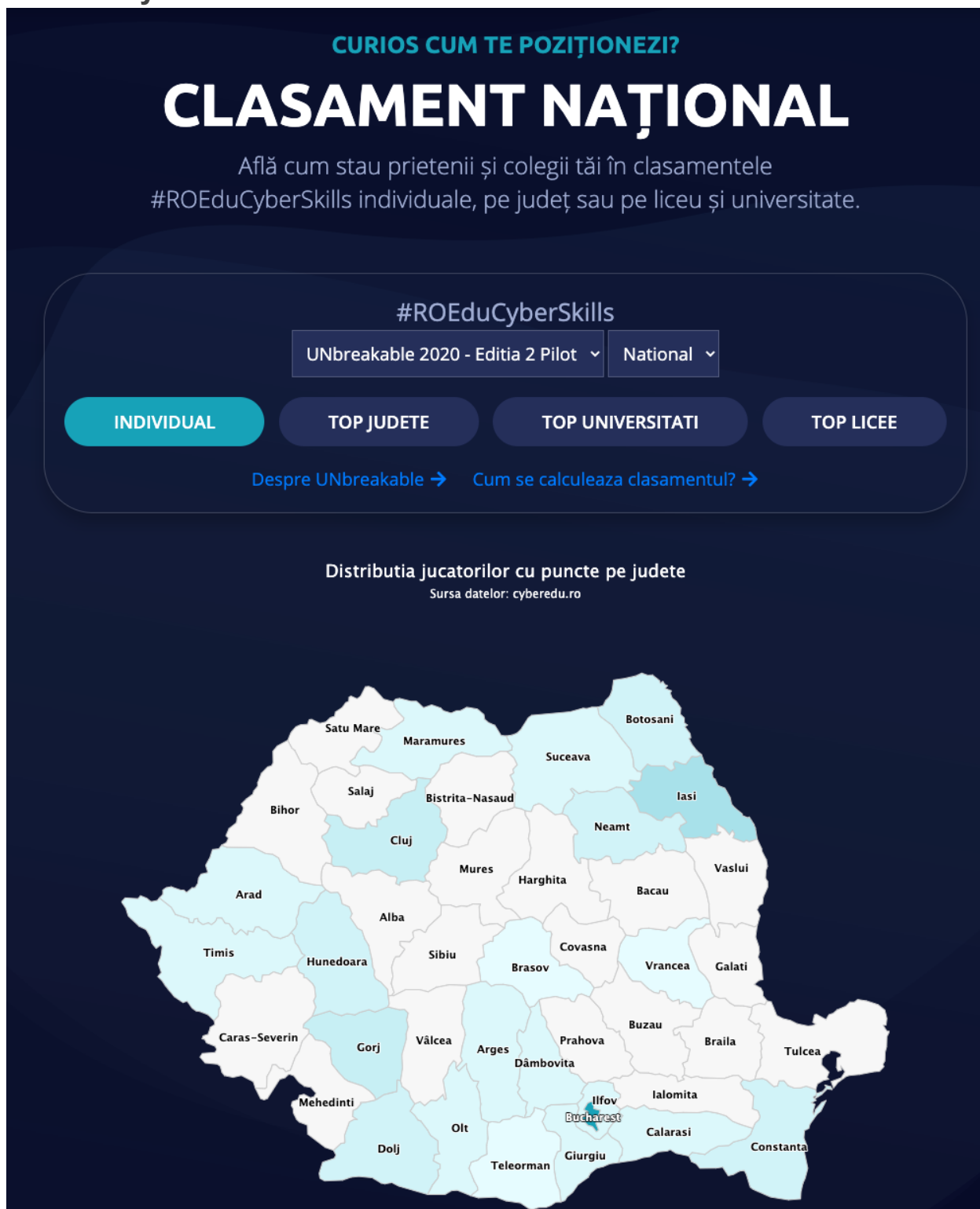
Scorul pe sezon

Scorul final pe sezon ia în considerare scorurile agregate din fiecare etapă de concurs. Scorul pe sezon va prezenta în mod individual rezultatele obținute pentru fiecare etapă dar și clasamentul final agregat pentru toate etapele de concurs.

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



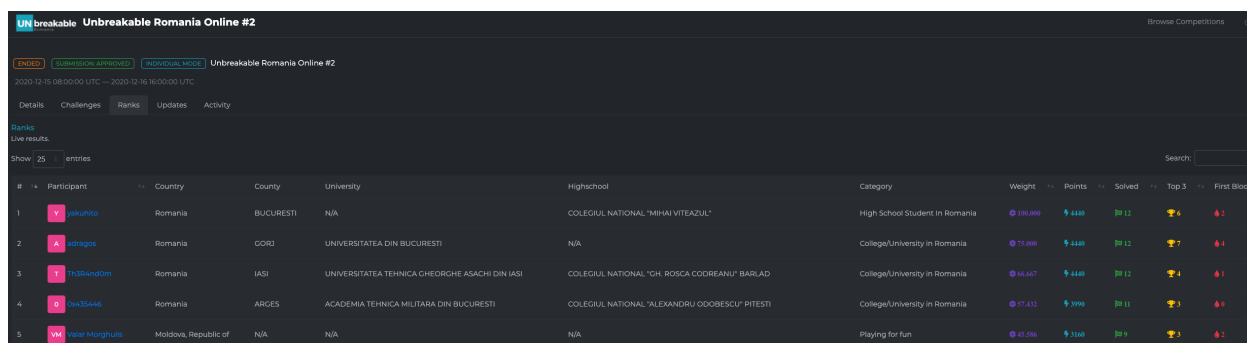
Fiecare județ, liceu sau universitate reprezentată va avea o poziție în clasamentul #ROEduCyberSkills pentru fiecare etapă, urmărindu-se următoarele aspecte:

- cel mai bine clasat jucător din etapa individuală
- cea mai bine clasată echipă din etapa pe echipe
- număr total de jucători înregistrați ce au obținut punctaj mai mare de 0 la etapa individuală
- punctajul mediu pentru jucătorii ce au obținut punctaj mai mare de 0 la etapa individuală

Un student poate contribui la #ROEduCyberSkills prin înregistrare și participare la etapa individuală, menționând instituția de învățământ de care aparține.

O echipă poate contribui la #ROEduCyberSkills prin participarea cu minim 1 jucător și maxim 3 jucători din aceeași instituție de învățământ. O echipă nu poate avea jucători din alte instituții de învățământ.

Ce este raportul individual de performanță?



#	Participant	Country	County	University	Highschool	Category	Weight	Points	Solved	Top 3	First Blood
1	Yakuhito	Romania	BUCURESTI	N/A	COLEGIUL NATIONAL "MIHAI VITEAZUL"	High School Student in Romania	100.000	4480	10/12	4	2
2	Astragos	Romania	GORJ	UNIVERSITATEA DIN BUCURESTI	N/A	College/University in Romania	71.000	4480	10/12	7	4
3	T03evadon	Romania	IASI	UNIVERSITATEA TEHNICA GHEORGHE ASACHI DIN IASI	COLEGIUL NATIONAL "GH. ROSCA CODREANU" BAILAD	College/University in Romania	66.667	4480	10/12	4	1
4	Dax30448	Romania	ARGES	ACADEMIA TEHNICA MILITARA DIN BUCURESTI	COLEGIUL NATIONAL "ALEXANDRU ODORSCU" PITESTI	College/University in Romania	57.431	5996	10/12	3	0
5	N04r H0ugh0u5	Moldova, Republic of	N/A	N/A	N/A	Playing for fun	45.506	3108	10/12	3	2

Fiecare jucător ce a participat atât la concursul individual cât și la cel pe echipe, va primi la finalul sezonului un raport individual de performanță detaliat. Raportul individual de performanță este conceput astfel încât să:

- informeze jucătorii despre punctele forte și punctele slabe
- demonstreze abilitățile tehnice în diverse medii (de exemplu la facultate, la angajare sau md)
- arate unui angajator potențialul și abilitățile pe care un jucător de la UNbreakable România le are
- prezintă detaliat, pe module rezultatele obținute de fiecare jucător
- evidențieze statisticile din fiecare sezon, modul de calcul, evoluția s.a.

Care sunt grupele în care poate fi încadrat un participant?

Fiecare jucător poate fi încadrat în una din grupele:

- **High School Student în România sau Elev**, tineri peste 16 ani ce sunt înscriși la un liceu din România

- **College / University in Romania sau Student**, studenți înscriși la o universitate din România

Cum se poate pregăti un participant pentru UNbreakable România?

Sezonul UNbreakable România de primăvară - vară 2021 debutează cu etapa de antrenament și pregătire. Participanții vor avea la dispoziție resurse teoretice și practice ce le va permite familiarizarea cu formatul și metodologia concursului. Se vor organiza webinarii cu experți în securitate cibernetică sau alumni din comunitate pe diverse subiecte de interes.

La sezonul UNbreakable primăvară-vară 2021, 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 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.

Categorii introductive

- Concepte fundamentale de securitate cibernetică
- Tehnologii pentru asigurarea securității cibernetică
- Tehnologii pentru identificarea vulnerabilităților
- Tehnologii de anonimizare
- Atacuri și tehnici de inginerie socială
- Managementul parolelor și tehnici de spargere a parolelor
- Participarea la programe de tip bug bounty
- Dezvoltarea unui business sau startup în securitate cibernetică

Categorii specializate

- Criptografie și algoritmi de criptare, encodare sau hashing

- Securitatea și exploatarea vulnerabilităților în aplicații web
- Securitatea și exploatarea vulnerabilităților în aplicații mobile / desktop
- Informațiile obținute pe baza tehnicilor și uneltelor de tip OSINT (Open Source Intelligence)
- Enumerarea și exploatarea serviciilor și sistemelor
- Analiza jurnale electronice (logs)
- Analiza traficului de rețea
- Analiza capturilor de date, memorie sau hard disk (forensics)
- Inginerie inversă pentru aplicații executabile, scripturi sau documente
- Securitatea rețelelor wireless

Care sunt oportunitățile de dezvoltare în afara de UNbreakable Romania pentru elevi si studenti?

Domeniul securității cibernetică este extrem de vast și există numeroase oportunități pentru a urma o cariera în industrie ca:

- **Penetration Tester** - Specialist în securitate informatică responsabil cu identificarea vulnerabilitatilor în sisteme informatice folosind tehnici cunoscute de hackeri
- **Analist in 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**
- Samd

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

- Campionatul European de Securitate Cibernetică - <https://www.cybersecuritychallenge.ro/>
- DefCamp Capture the Flag - <https://dctf.def.camp/>
- HackTM - hacktm.ro/
- X-MAS CTF - <https://htsp.ro/>
- Anual pe platforma <https://cyberedu.ro> sunt anuntate si organizate si alte evenimente ad-hoc

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 amd)
- 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.

Exerciții și rezolvări

Warm-UP Individual

Concurs UNbreakable 2021 #Individual

Descriere:

The best secrets agents from D.O.D are being interviewed with some knowledge-based questions before having the technical tests, so are you ready?

Rezolvare:

Q1: Ce tip de control este implementarea unui firewall?

Format flag: tehnic

Q2: Cum se numește tehnologia cea mai populară ce este folosită în a identifica manual vulnerabilități de Wordpress?

Format flag: WPscan

Q3: Ce factor biometric reprezinta un identificator unic per utilizator , ce este foarte des folosit în zilele noastre, mai ales în cazul aparaturilor mobile?

Format flag: amprenta

Q4: Cum se numește “inima” sistemului de operare?

Format flag: kernel

Q5: Ce metoda putem folosi pentru a insera valori intr-un sir de text?

Format flag: format string

Q6: Ce metoda de protectie putem folosi în a împiedica exploatarea vulnerabilităților ce țin de memoriile corupte aferente programelor targetate?

Format flag: ASLR

Q7: Cum numim vulnerabilitatea prin care un program este forțat să execute două sau mai multe funcții în același timp?

Format flag: race condition

Q8: Cum se numește metoda de protectie aplicată unui binar, ce face ca valorile din memorie să primească alta adresa de fiecare data cand acesta este lansat?

Format flag: PIE

Q9: Cum se numește procesul prin care un atacator sau un hacker etic poate ascunde un mesaj secret în interiorul unui mesaj vizibil, fara a putea fi interceptat?

Format flag: stenografie

Q10: Care este una dintre cele mai utilizate unelte pentru a ascunde mesaje în interiorul imaginilor și a fișierelor de tip .pdf?

Format flag: exiftool

Q11: Ce extensie are o aplicație specifică pentru platforma iOS?

Format flag: ipa

Q12: Cine a realizat primul jailbreak software pentru sistemul de operare iOS?

Format flag: Saurik

Q13: Ce aplicație înlocuiește AppleStore, după ce un atacator conduce un proces de jailbreak pe un aparat mobil ce are instalat iOS OS? Ține cont că această aplicație este necesară utilizatorului rău intenționat pentru a și instala unelte de atac pentru aparatul țintă?

Format flag: Cydia

Q14: Ce instrument pentru platforma Linux putem folosi atunci când căutăm un set specific de date în procesul de analiză a unui binar?

Format flag: grep

Q15: Cum numim un set de date ce poate avea doar valorile: "true" sau "false"?

Format flag: boolean

Q16: Cum se numește procesul prin care se extrag fișiere cu conținut critic sau fișiere ce au fost șterse dintr-un mediu de stocare, atunci când analizăm un incident informatic?

Format flag: disk forensics

Q17: Cu ce software putem analiza un fișier audio?

Format flag: Audacity

Q18: Ce tip de program poate folosi un atacator pentru a evita procesul de autentificare într-un sistem țintă?

Format flag: backdoor

Q19: Ce componenta este datoare într-o rețea de calculatoare să transmită pachete de date între două sau mai multe calculatoare?

Format flag: router

Q20: În utilizarea carui algoritim este necesara o matrice de 5x5 pentru substituirea fiecărei litere din alfabet?

Format flag: PlayFair

Q21: Ce cipher are la baza tehnica Tabula recta inventata in 1508 de Johannes Trithemius?

Format flag: Beaufort

Q22: Ce protocol reprezinta baza de comunicare pentru World Wide Web?

Format flag: HTTP

Q23: Ce termen folosim atunci cand vorbim despre adresele web, care specifică și protocolul utilizat la trimiterea / primirea informațiilor?

Format flag: URL

Q24: Ce metodologie este cea mai des folosită atunci cand un hacker etic conduce un test de tip black-box penetration?

Format flag: OWASP

Social-Agency (Hard)

Concurs UNbreakable 2021 #Individua

Autor exercițiu: Lucian Nițescu

Contribuitori rezolvare: Niță Horia & Valentina Galea

Descriere:

Dear Agent, as your first task within the Agency, find the last known location of tecgirwilliam@gmail.com also called Tecgir William without attempting to hack or brute force within any account. All information is of course public. After that maybe we can have that call over Google Hangouts/Meets (or both) about how to clean the cafeteria.

Note: The flag of this code must be generated as such: CTF{sha256sum('Google Plus Code')}

Rezolvare:

În enunțul problemei, primim adresa de e-mail și numele suspectului.

EMAIL: tecgirwilliam@gmail.com
NAME: Tecgir William

Există, de asemenea, ceva legat de Google Hangouts.

Am mai văzut astfel de probleme înainte, așa că am folosit pur și simplu GHunt pentru a-mi rezolva toate problemele. Am descărcat GHunt de pe GitHub, am setat cookie-urile și apoi am rulat `python3 ghunt.py email tecgirwilliam@gmail.com`. Acest lucru mi-a dat următorul rezultat:

```
Name : Tecgir William
[-] Default profile picture
Last profile edit : 2021/12/02 08:42:10 (UTC)
Email : tecgirwilliam@gmail.com
Google ID : 111076247952673225160
Hangouts Bot : No
[+] Activated Google services :
- Hangouts
[-] YouTube channel not found.
Google Maps : https://www.google.com/maps/contrib/111076247952673225160/reviews
[+] 1 reviews found !
[+] Average rating : 5/5 stars !

[+] Probable location (confidence => Very low) :
- Călimănești, România
Google Calendar : https://calendar.google.com/calendar/u/0/embed?src=tecgirwilliam@gmail.com [-] No public Google Calendar.
```

Vedem că are o recenzie publicată pe contul său de gmail. După ce vizităm link-ul Google Maps, vedem că a lăsat o recenzie de 5 stele pentru Cascada Lotrisor. Apăsând pe butonul DETALIILE LOCULUI, găsim codul Google Plus al locului (872J+WX Brezoi).

Îl luăm și executăm următorii pași:

```
echo -n "872J+WX Brezoi" |sha256sum .
```

După ce am făcut acest lucru, obținem un șir sha256sum pe care o înfășurăm în CTF{}, și acesta este steagul nostru.

```
CTF{e0c34f6ffe1dcc87c67a4f[REDACTAT]1871ea7afcb49e55b81257d}
```

Basic-ics (easy)

Concurs UNbreakable 2021 #Echipe

Autor exercițiu: Andrei Avădănei

Contribuitori rezolvare: Andrei Albișoru, Teodor Duțu, Adina Smeu, Valentina Galea

Descriere:

Vei primi o serie de întrebări, unele cu variantă unică de răspuns, altele cu variante multiple. Peste punctajul de trecere vei primi flagul.

Link chestionare:

Warmup: <https://infosec-ro.typeform.com/to/J2ecyWwZ>

P1: <https://infosec-ro.typeform.com/to/hirA6sOs>

P2: <https://infosec-ro.typeform.com/to/nO8axwCX>

Resurse utile: înregistrarea webinarului realizată de Albert Vartic, din partea OMV Petrom + resursele din Bootcamp publicate de acesta în secțiunea de pe Google Drive.

Rezolvare:

Felicitari, ai obținut 100!

Flagul este

```
CTF{82ec99615648626454a5c6696b1721ffbd14597d9e1b2a1da6acee5da5b3b808}
```

Care din protocoalele de mai jos sunt folosite la Nivelul Dispozitivelor (Instrumentației) din Câmp?

A Foundation Fieldbus

B 4-20mA

C Ethernet/IP

D HART

Care este rolul HMI-urilor?

A Servesc ca interfața grafică între Sistemele de Control și Operator

B Se folosesc pentru conferințele video între angajații companiei

C Reprezintă grafic procesele care sunt controlate de sisteme de control

D Pentru vizualizarea materialului de training pentru sistemele de control

La ce servesc Sistemele de Siguranță?

A Sunt sistemele care devin colorate în roșu în caz de atac cibernetic

B Reprezintă sistemele care intervin când sistemul de control de bază a procesului nu face față

C Ajută operatorii să poată ieși din instalații în cazuri de urgență

D Sunt sistemele care asigură un nivel de protecție suplimentară

O buclă de control în un sistem de control Industrial este alcătuită din?

A Element Inițial - Controller - Element final

B Controller - Element Inițial - Element Final

C Controller - Operator - Element Inițial

D Operator - Controller - Element de execuție

În Modelul Purdue Dispozitivele (Instrumentele) de câmp la care nivel se regăsesc?

A Nivel 3

B Nivel 4

C Nivel 0

D Nivel 2

E Nivel 1

Ce înseamnă Industria 4.0?

A Securitate Informatică la revizia 4

B Nivelul 4 de dezvoltare a Industriei în lume

C Un soft pentru Securitatea Cibernetică

D Sistemul Național de Informare despre Securitatea Cibernetică

Pentru care din cazurile de mai jos sunt folosite Firewall-urile în OT/ICS?

A Pentru izolarea dispozitivelor (instrumentelor) de câmp de la scurtcircuit

B Pentru protejarea perimetrală a zonelor din rețelele TCP/IP

C Dispozitive pentru protecția zidurilor

D Pentru a bloca curentul între controller și elementele finale

În ce scopuri este folosită o Stație de Inginerie?

A Pentru a da posibilitate Inginerului de Sisteme să facă modificări în setările sistemelor de control

B Pentru a folosi AutoCAD-ul și MS Office

C Pentru a ține evidența inginerilor din o instalație

D Pentru a comunica cu sistemele ERP

Care sunt cele mai importante 2 priorități în Securitatea Cibernetică din OT?

A Disponibilitatea și Confidențialitate

B Confidențialitate și Integritate

C Integritate și Confidențialitate

D Siguranța și Disponibilitate

Modelul feliilor de cașcaval cu ce poate fi asociat?

A Cu un model de scări ierarhice

B Cu un model de bariere de protecție

C Cu procesul de certificare a operatorilor

D Cu procesul de verificare a sistemelor de control

În Modelul Purdue este conectat direct la Internet următorul nivel

A Nivel 3

B Nivel 5

C Nivel 2

D Nivel 4

E Nivel 0

F Nivel 1

Care din următoarele afirmații despre protocoalele industriale în general este corectă?

A Protocoalele industriale oferă întotdeauna posibilitatea unei implementări sigure, dar acest lucru nu este de obicei utilizat din cauza eforturilor suplimentare de configurare.

B Protocoalele proprietare sunt rareori găsite în lumea OT, deoarece aproape toate protocoalele sunt open source.

C Pe parcursul dezvoltării protocoalelor industriale disponibilitatea sistemelor de control a fost scopul principal și caracteristicile de securitate au fost adăugate doar în versiunile mai noi.

D Versiunile mai noi și sigure ale protocoalelor industriale sunt întotdeauna acceptate de toate componentele sistemelor de control, inclusiv componente vechi.

La folosirea protocolului Modbus RTU prin RS-485 IP-urile lui Master și Slave trebuie să fie din aceeași clasă?

A Da

B Da, doar dacă sunt separate prin un switch de rețea

C Nu are relevanță - nu se folosesc IP la acest tip de comunicație

D Nu, pot fi din clase diferite

Care este relația dintre Nivelul de Protecție și Risc în OT/ICS?

A Nivelul de Protecție determină Riscul doar când avem o amenințare

B Riscul este parte componentă a Nivelului de Protecție

C Riscul este invers proporțional cu Gradul Nivelului de Protecție

D Nivelul de Protecție este întotdeauna mai mare ca Riscul

La ce se referă Cerințele Fundamentale în Standardul IEC-62443-1-1/3-3?

A Sunt cerințe care trebuie îndeplinite în vederea certificării ca specialist în Securitate Cibernetică OT

B Sunt cerințele de bază care trebuie respectate pentru asigurarea securității ICS

C Sunt cerințe de proiectare a unui Element final din bucla de control

D Sunt 5 cerințe ce trebuie respectate de fiecare dată când pornim un PLC

Câte nivele de securitate (SL) sunt definite în IEC-62443?

A 7

B 4

C 6

D 3

În ce constă conceptul Defense-in-depth?

A Constă în descrierea soluției de securitate în adâncime în companii unde nu sunt rețele

B Un concept de aplicare a mai multor măsuri de securitate pe nivele și în pași

C Include doar echipamentele din rețea

D Este noțiunea despre cum trebuie protejate PLC-urile când nu sunt în rețea

Ce conține conceptul de ICS Cyber Kill Chain?

A Conține elemente din ICS, care nu au protecție

B Este o metoda de a atrage atacatorii

C Cuprinde etapele de proiectare a unui ICS

D Un concept care explică pașii prin care trece un adversar executând un atac asupra ICS

Care sunt principalele 3 componente ce determină Securitate Cibernetică în OT/ICS

A Procese - Tehnologii - Oamenii

B Tehnicienii - Inginerii - Procese

C Oamenii - Tehnologii - Procesoare

D Procese - Oamenii - Siguranța

Cum sunt denumite comenzile în protocolul Modbus?

A Registre

B Coil

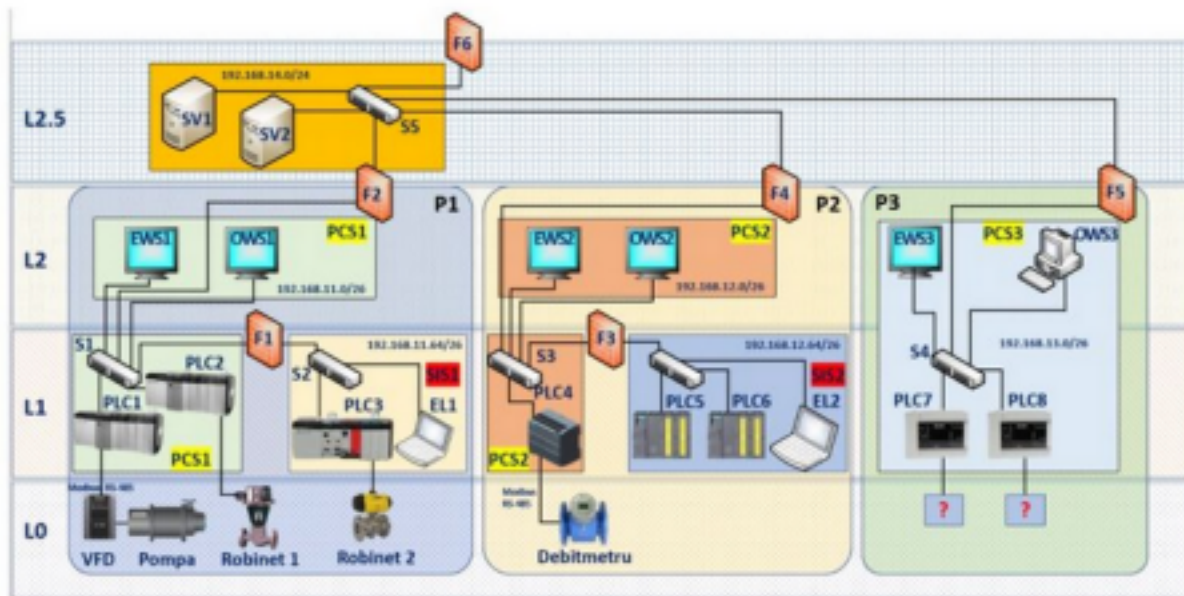
C Controale

D Funcții

P1

Felicitari, ai obtinut punctajul 60!

Flagul este CTF{fab95cbd3a53077a6807cac[REDACTAT]2f07eac3d7d25fa3ff5e2}



Nota: Toate datele din arhitectura ICS sunt conform cu scenariile descrise in exercitii.

Legenda

Abr	EN	RO
PCS	Process Control System	Zona Sistemului de Baza de Control
SIS	Safety Integrated System	Zona Sistemului de Siguranta
PLC	Programmable Logic Controller	Controler Logic Programabil
EL	Engineering Laptop	Laptop de Inginerie
S	Network Switch	Switch de Rețea
OWS	Operator Work Station	Stație de Lucru Operator
EW	Engineering Work Station	Stație de Lucru Inginer
VFD	Variable Frequency Driver	Variator de Frecvență
P	Plant	Facilitate de Producție
F	Firewall	Firewall
SV	Server	Server

Din capturile de trafic au fost extrase următoarele informații:

```
Ethernet II, Scr: 04:0e:3c:12:a1:5e, Dst: XX:XX:XX:XX:XX:XX  
Internet Protocol Version 4, Scr: 192.168.11.69, Dst: 192.168.11.68  
Transmission Control Protocol, Scr Port: 60112, Dst Port: 44818, Seq: 155, Ack:122, Len:65
```

- Se știe că EWS1 și OWS 1 au același producător - DELL
- Din SIS1 doar PLC3 comunica cu OWS 1
- Din P1 doar OWS 1 comunica cu L2.5
- Toate PLC-urile au doar câte 1 port de comunicare (de tip Ethernet) în zonele PCS și SIS

Care este IP-ul lui EL1?

- A 192.168.11.68
- B 192.168.11.69**
- C 192.168.11.63
- D 192.168.11.129

Care este Producătorul lui EL1?

- A Fujitsu
- B HP**
- C Acer
- D Asus
- E DELL
- F Fujitsu-Siemens

Care este IP-ul lui EWS1?

- A 192.168.11.42**
- B 192.166.11.12
- C 192.186.11.4
- D 192.168.12.34

Care este IP-ul lui OWS 1?

- A 192.158.11.32
- B 192.168.11.41**
- C 192.168.10.12
- D 192.168.11.65

Care este IP-ul lui PLC1?

- A 192.168.11.24**
- B 192.168.10.12
- C 192.168.11.66
- D 192.158.11.32

Care este Modelul lui PLC1?

A ControlLogix 5570

B Twido

C S7-1500

D iQ-R

E SLS 1508

F MasterLogic ML200

Care este IP-ul lui PLC3?

A 192.168.11.82

B 192.166.11.12

C 192.168.10.25

D 192.168.11.68

Care este Modelul lui PLC3?

A SLC 500

B ControlLogix 5580

C S7-1200

D MELSEC-F

E LOGO!

F GuardLogix 5570

Prin ce protocol comunica EL1 cu PLC3?

A Modbus TCP/IP

B EtherNet/IP

C DNP3

D OPC DA

E Profinet

Variatorul de Frecventa comunica cu PLC 1 prin comunicație serială Modbus RS-485.

Care poate fi IP-ul asignat VFD-ului?

A 192.168.10.25

B 192.178.11.32

C Niciuna

D 192.168.11.27

PLC2 da o comanda de deschidere Robinet 1 la starea de 75% deschis (100% fiind total deschis = 20mA). Care va fi valoare ieșirii analogice operându-se cu 4-20mA?

A 8 V

B 8 mA

C 10 mA

D 16 mA

În caz de Emergenta PLC3 trebuie sa deschidă Robinetul 2. In cazul in care avem lipsa alimentare electrica la PLC3 și nu tine nici UPS-ul, ce se va întâmpla cu Robinetul 2?

A Se va Închide

B Va rămâne în starea sa inițială - închis.

C Se va deschide

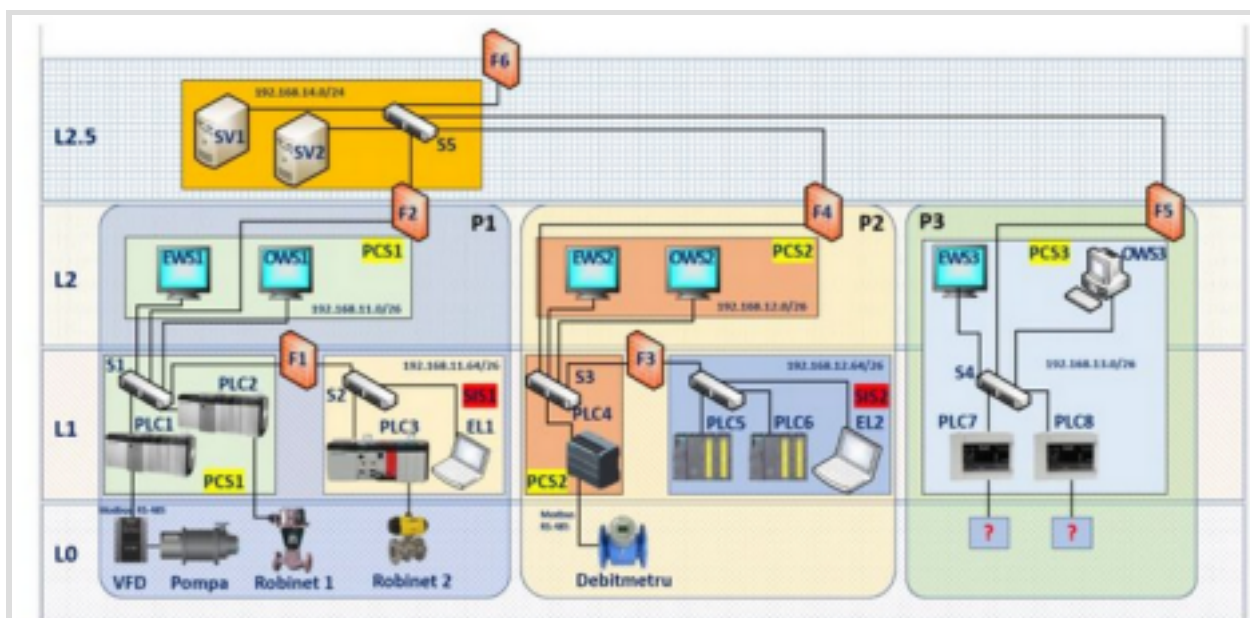
D Va sta închis până când revine alimentarea electrica la PLC3

P2

Felicitari, ai obtinut punctajul 50!

Flagul este

CTF{d1288f4c083add6f8cfe76498dea5695696390e420f3870356268cc006d46610}



Nota: Toate datele din arhitectura ICS sunt conform cu scenariile descrise in exerciții.

Legenda

Abr	EN	RO
PCS	Process Control System	Zona Sistemului de Baza de Control
SIS	Safety Integrated System	Zona Sistemului de Siguranță
PLC	Programmable Logic Controller	Controller Logic Programabil
EL	Engineering Laptop	Laptop de Inginerie
S	Network Switch	Switch de Rețea
OWS	Operator Work Station	Stație de Lucru Operator
EWS	Engineering Work Station	Stație de Lucru Inginer
VFD	Variable Frequency Driver	Variator de Frecvență
P	Plant	Facilitate de Producție
F	Firewall	Firewall
SV	Server	Server

Din capturile de trafic au fost extrase următoarele informații:

Ethernet II, Scr: 00:1d:09:99:b2:2c, Dst: XX:XX:XX:XX:XX:XX
Internet Protocol Version 4, Scr: 192.168.12.69, Dst: 192.168.12.71
Transmission Control Protocol, Scr Port: 61246, Dst Port: 102, Seq: 145, Ack:112, Len:32

- Se știe ca EWS2 si OWS 2 au același producător - HP
- Din SIS2 doar PLC 5 comunica cu OWS2
- Din P2 doar OWS 2 comunică cu L2.5
- Toate PLC-urile au doar cate un port de comunicare (de tip Ethernet) in zonele PCS si

SIS

Care este IP-ul lui EL2?

A 192.168.12.129

B 192.168.12.69

C 192.168.12.68

D 192.168.12.71

Care este Producătorul lui EL2?

A Fujitsu-Siemens

B HP

C Asus

D Acer

E DELL

F Fujitsu

Care este IP-ul lui

EWS2? A 192.186.12.42

B 192.166.12.12

C 192.168.12.34

D 192.168.11.34

Care este IP-ul lui OWS2?

A 192.168.12.55

B 192.168.11.12

C 192.186.12.41

D 192.168.12.82

Care este IP-ul lui

PLC5? **A 192.168.12.72**

B 192.158.12.32

C 192.168.12.24

D 192.186.12.12

Care este Modelul lui PLC5?

A MasterLogic ML200

B ControlLogix 5570

C Twido

D S7-1200

E S7-300F

F SLS 1508

Care este IP-ul lui
PLC4? A 192.186.12.12
B 192.186.12.12
C 192.158.12.23
D 192.168.12.24

Care este Modelul lui PLC4?
A S7-1200
B SLC 500
C LOGO!
D GuardLogix 5570
E MELSEC-F
F S7-1500

Prin ce protocol comunica EL2 cu PLC6?
A DNP3
B EtherNet/IP
C OPC DA
D Modbus TCP/IP
E S7

Debitmetrul comunica cu PLC4 prin comunicație seriala Modbus RS-485. secvența de
interogare citire valoare debit de la debitmetru care fa fi Numele Funcției?
A 3
B 1
C 2
D 5

Eyewitness (mediu)

Concurs UNbreakable 2021 #Echipe

Autor exercițiu: Antonio Macovei (ZNQ)

Contribuitori rezolvare: Andrei Albișoru, Teodor Duțu, Adina Smeu, Valentina Galea

Descriere:

We have just identified an important new eyewitness in a murder **case**, but they can't seem to remember where they were when it happened. We just know that they were drinking a coffee and watching out the window from across the street. They had the 3rd room on the corridor, on the 3rd floor. It is very important that we identify the EXACT location, with a very high accuracy (about 3 square meters), so our team can establish the witness' point of view of the crime scene. Failing to **do** so will allow the criminal to walk free.

Check the attached photo, it might contain some clues.
Flag format: CTF{SHA256(location)}

Rezolvare:

Trebuie să găsim un site care să aibă legătură cu 3 și locații, așa că am căutat pe internet până am găsit <https://what3words.com> cu interogarea maps location 3 (după ce am încercat latitudine și longitudine, Google Plus Code etc.).

Locația din fotografie este Casa Capsa.

Din moment ce în descriere se spunea că martorul ocular se afla vizavi, asta înseamnă că se află fie în Hotel Capitol, fie în Old City Gem.

Era lângă o fereastră, așa că am extras toate pătrățelele care păreau a fi lângă una din cele 2 clădiri anterioare:

```
#Capitol
majority.print.flipping
nickname.intervals.quite
agenda.changing.magnets
walkway.ropes.lined
song.oasis.walled
without.done.collects
showdown.thumps.cake
electric.decay.monitors
mimed.resides.bribing
napkins.host.anyone
officer.scale.obey
says.pouch.nearing
greeting.visual.stables
locals.fevered.drips
ridge.gliding.terms
dish.protect.lowest
trumped.directs.altering
#Old
assure.courage.point
divide.turned.layered
book.shoebox.passes
dispose.flicks.duck
runs.gallons.talker
wagers.struck.proven
bared.actual.elated
audible.claps.zoomed
players.left.roofer
```

```
suitable.influencing.observer  
tanked.pigs.delved  
mass.bunkers.sweeping  
devotion.evaded.will  
collects.happy.purple  
exhale.spill.wasp  
voter.necklace.pushed  
nappy.helpless.attracts
```

Apoi am generat toate steagurile posibile:

```
from hashlib import sha256  
  
locations = open('locations.txt').read().split()  
  
for loc in locations:  
    v = '///'+loc  
    print(v)  
    if len(loc) == 0 or loc[0] == '#':  
        continue  
  
    m = sha256()  
    m.update(v.encode())  
  
    print(f'CTF{{{m.digest().hex()}}})
```

Rise (ușor)

Concurs UNbreakable 2021 #Echipe

Autor exercițiu: Răzvan Deaconescu

Contribuitori rezolvare: Andrei Albișoru, Teodor Duțu, Adina Smeu, Valentina Galea

Descriere:

```
Get the flag by authenticating via SSH to ctf@159.223.26.66 -p4556, using the password  
"d4rk_kn1ght".
```

Rezolvare:

Folosim ssh să ne conectăm la mașina:

```
ssh ctf@159.223.26.66 -p 4556
```

Începem să căutăm binare:

```
ctf@73007e61b6eb:~$ find / -uid 0 -perm -4000 -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/ping6
/bin/umount
/bin/su
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/power
/usr/lib/openssh/ssh-keysign
```

Folosim scp pentru a obține binarul power

```
adina@asm:rise$ scp -P 4556 ctf@159.223.26.66:/usr/bin/power .
ctf@159.223.26.66's password:
power 100% 6120
163.6KB/s 00:00
```

Am inspectat apoi binarul cu Ghidra și am observat câteva funcții:

- 0x001008ea - inversează un șir de caractere
- 0x00100950 - citește un caracter la o anumită poziție dintr-un fișier dat
- 0x00100a07 - apelează cele 2 funcții menționate mai sus

Aceasta însemna că executabilul primea ca argument numele inversat al fișierului din care dorim să citim și un index al caracterului.

Apoi, am folosit bash pentru a citi steagul, caracter cu caracter și am obținut soluția:

```
ctf@73007e61b6eb:~$ flag=""
ctf@73007e61b6eb:~$
ctf@73007e61b6eb:~$ for i in {0...
50}
> do
>     crt_char="$(power galf $i)"
>     flag=$flag$crt_char
> done
ctf@73007e61b6eb:~$
ctf@73007e61b6eb:~$ echo $flag
```


Contribuitori

- Florina Dumitrache
- Niță Horia
- Valentina Galea (Volf)
- Andrei Avadanei
- Monica Obogeanu
- Andrei Albișoru
- Teodor Duțu
- Adina Smeu