Ministerul Educaţiei, Culturii și Cercetării

Universitatea Tehnică a Moldovei

Faculatea Calculatoare, informatică și microelectronică  
Departamentul Ingineria Software și Automatică



**RAPORT**

Lucrare de Laborator nr.3

Proiectarea sistemelor informaționale

A efectuat:

Chihai Adrian

A verificat:

Magdei Octavian

Chişinău 2025

# Descrierea procesului ales

Procesul selectat pentru realizarea acestei lucrări de laborator reprezintă procesul de analiză și implementare a tehnicilor brute-force pentru cracking-ul hash-urilor. Acesta este conceput pentru a evalua vulnerabilitățile sistemelor de securitate bazate pe algoritmi de hashing și pentru a oferi soluții practice și eficiente. Este un instrument valoros pentru profesioniștii în securitate cibernetică, deoarece le oferă posibilitatea de a înțelege mai bine limitele algoritmilor de hashing și de a dezvolta soluții pentru prevenirea accesului neautorizat.

Acesta poate implica următorii pași:

* analiza tehnicilor brute-force;
* determinarea tipului de hash;
* implementarea algoritmilor brute-force pentru decriptarea hash-urilor;
* optimizarea procesului de cracking;
* testarea eficienței tehnicilor brute-force;
* generarea rapoartelor de performanță.

Unul dintre primii pași este analiza tehnicilor brute-force, unde se selectează metodele aplicabile pentru cracking-ul diferitelor tipuri de hash-uri (MD5, SHA-1, SHA-256). După aceasta, utilizatorul poate introduce hash-ul țintă, iar aplicația determină automat tipul acestuia. Acest pas este crucial pentru alegerea algoritmului potrivit și creșterea eficienței procesului.

După determinarea tipului de hash, algoritmii brute-force sunt implementați pentru decriptare, utilizând wordlist-uri optimizate. Acest proces presupune generarea și verificarea unui număr mare de combinații de parole până la găsirea uneia care corespunde hash-ului introdus. Pe parcurs, aplicația optimizează procesul prin reducerea spațiului de căutare și utilizarea unor tehnici precum preprocesarea datelor sau utilizarea hardware-ului accelerat, cum ar fi GPU-uri.

Procesul de cracking generează date esențiale, precum timpul de execuție și rata de succes. Acestea sunt incluse într-un raport detaliat care ajută utilizatorul să înțeleagă eficiența tehnicilor aplicate. În plus, aplicația oferă o interfață grafică intuitivă (GUI), care permite utilizatorilor să acceseze funcționalitățile fără a necesita cunoștințe avansate în securitate cibernetică.

Procesul de analiză și implementare a tehnicilor brute-force pentru cracking-ul hash-urilor contribuie la o mai bună înțelegere a vulnerabilităților asociate algoritmilor de hashing. Este un instrument esențial pentru profesioniștii din domeniu și ajută la identificarea măsurilor de protecție pentru îmbunătățirea securității datelor.

# 2. Elaborarea unui model logic al datelor pentru procesul ales

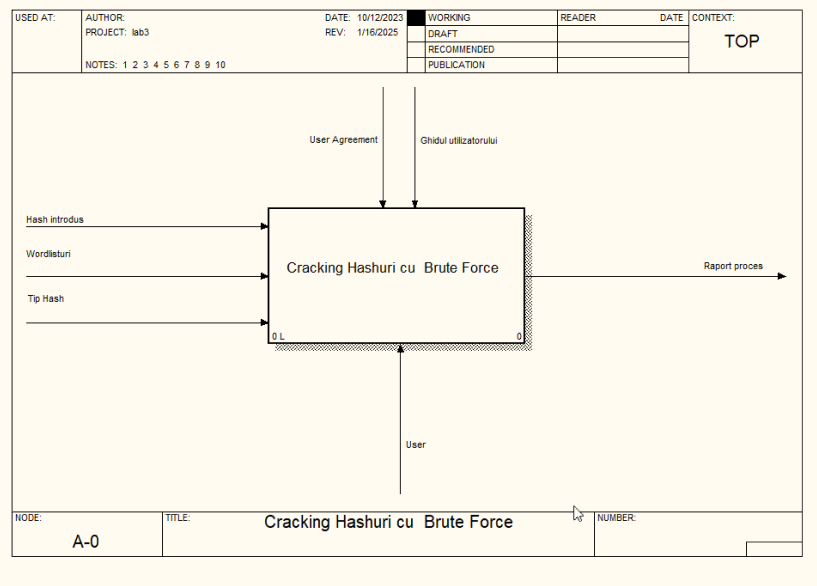


Figura 2.1 – Diagrama de context

Diagrama de context reprezentată în figura de mai sus oferă o viziune de ansamblu asupra procesului de cracking hash-uri cu brute force. Pentru realizarea acestui proces, utilizatorul trebuie să introducă un hash țintă. De asemenea, este necesară furnizarea unui wordlist și, opțional, a tipului de hash, pentru a facilita aplicarea tehnicii brute-force în mod eficient.

Procesul este ghidat de instrucțiuni clare oferite prin intermediul aplicației, sub forma unui ghid al utilizatorului. Pe parcurs, utilizatorul este informat despre progresul procesului și poate vizualiza rapoarte detaliate despre performanța și eficiența tehnicilor aplicate.

Rezultatul acestui proces constă în:

* Determinarea parolei asociate hash-ului furnizat;
* Generarea unui raport detaliat cu timpul de execuție, numărul de combinații testate și rata de succes;

O mai bună înțelegere a vulnerabilităților algoritmilor de hashing folosiți.

Această diagrama subliniază elementele-cheie necesare pentru a facilita procesul și rolul utilizatorului în inițierea și monitorizarea cracking-ului hash-urilor.

# 2.1 Diagrama IDEF0

Diagramele IDEF0, cunoscute sub denumirea de Integration Definition for Function Modeling, reprezintă un instrument esențial în domeniul ingineriei sistemelor și ingineriei software, folosit pentru a modela și analiza funcțiile și procesele din cadrul sistemelor complexe. Aceste diagrame au ca scop să ofere o reprezentare vizuală a structurii, funcțiilor, interacțiunilor și relațiilor dintre elementele care alcătuiesc un sistem sau proces specific.

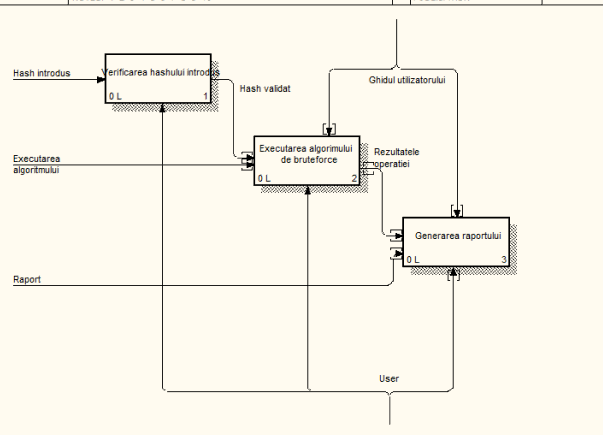
****

Figura 2.2 – Diagrama IDEF0

Diagrama IDEF0 care poate fi observată în figura 2.2 prezintă o reprezentare detaliată a procesului de **cracking al hash-urilor cu brute-force**. În primul rând, hash-ul introdus de utilizator este verificat pentru a asigura validitatea și compatibilitatea acestuia cu algoritmii disponibili. După validare, are loc procesul de executare a algoritmului de brute-force, utilizând datele furnizate, precum wordlist-uri și tipul hash-ului.

Rezultatele operației, incluzând statusul și eficiența algoritmului aplicat, sunt transmise utilizatorului. În etapa finală, un raport detaliat este generat, conținând informații despre timpul de execuție, parolele testate și succesul operației. Această diagramă evidențiază interacțiunea dintre utilizator, algoritm și aplicație, oferind o imagine clară a procesului etapizat.

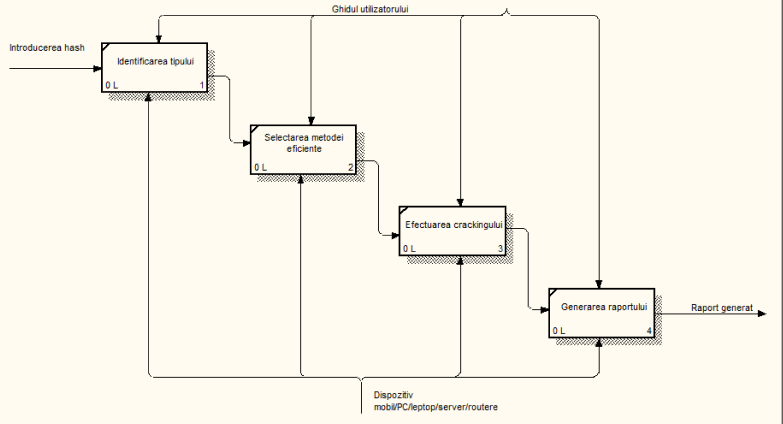


Figura 2.3 – Diagrama IDEF1

În figura de mai sus putem observa o reprezentare detaliată a procesului de cracking al hash-urilor. Acesta implică mai multe etape bine definite:

* Identificarea tipului de hash: Utilizatorul introduce hash-ul, iar sistemul determină automat tipul acestuia pentru a selecta algoritmul adecvat.
* Selectarea metodei eficiente: Sistemul alege metoda optimă de brute-force în funcție de tipul hash-ului și resursele disponibile.
* Efectuarea cracking-ului: Algoritmul selectat este aplicat, utilizând wordlist-uri și alte tehnici de optimizare pentru a găsi parola corespunzătoare hash-ului introdus.
* Generarea raportului: La final, un raport detaliat este generat și prezentat utilizatorului, incluzând informații despre timpul de execuție, eficiența metodei aplicate și rezultatele procesului.

Acest proces este ghidat de interfața utilizatorului (GUI) și poate fi realizat pe diferite dispozitive, precum laptopuri, servere sau alte echipamente dedicate. Raportul generat oferă utilizatorului o imagine completă asupra performanței și eficienței cracking-ului.

# 2.2 Diagrama IDEF3

Scopul principal al diagramei IDEF3 este de a captura detaliile proceselor, inclusiv fluxurile de date, obiectivele, activitățile și relațiile dintre acestea. Prin intermediul acestei metodologii, se realizează o descriere comprehensivă a proceselor, ceea ce facilitează analiza și evaluarea acestora.

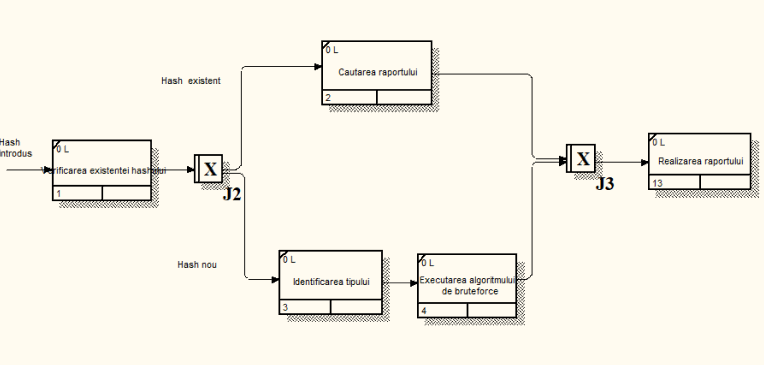


Figura 2.4 – Diagrama IDEF3

Diagrama din figura de mai sus este una de tip IDEF3 care reprezintă procesul de verificare a existenței unui hash. Dacă hash-ul introdus există, se caută raportul asociat. În caz contrar, are loc identificarea tipului de hash, executarea algoritmului de brute-force și generarea unui raport nou.

# 2.3 Diagrama DFD

Diagrama Fluxului de Date (DFD) este o tehnică grafică utilizată pentru modelarea, analiza și documentarea proceselor și fluxurilor de date într-un sistem sau organizație. Această tehnică este utilizată pe scară largă în domeniul dezvoltării software, în ingineria sistemelor și în managementul proceselor pentru a oferi o înțelegere clară a modului în care datele și informațiile circulă în cadrul unui sistem sau organizație.Scopul unei diagrame DFD este de a ilustra fluxurile de date și procesele într-un sistem sau organizație.

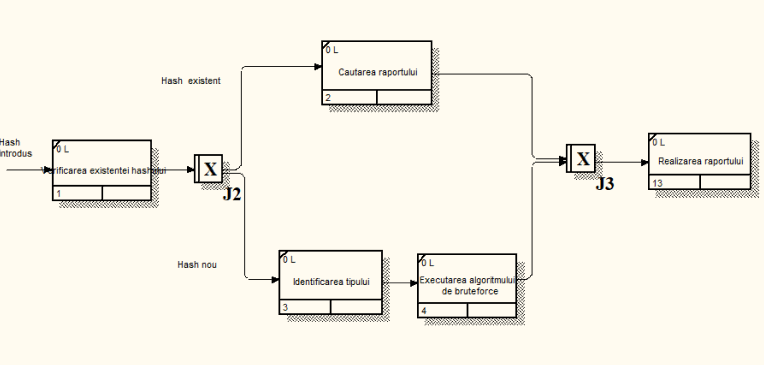
****

Figura 2.5 – Diagrama DFD

În ultima figură putem observa diagrama DFD pentru adăugarea hashului pentru cracking. În cazul dat aceasta ilustrează fluxurile de procese și date pentru procesul enunțat mai sus.

# CONCLUZII

Realizarea diagramelor IDEF0, IDEF1x și DFD în cadrul proiectului de dezvoltare a aplicației pentru cracking-ul hash-urilor a demonstrat importanța acestor instrumente în modelarea, analiza și proiectarea proceselor și datelor implicate. Aceste diagrame au fost esențiale pentru a obține o înțelegere comprehensivă a funcționării aplicației și a relațiilor dintre diferitele sale componente.

Diagramele IDEF0 au oferit o perspectivă globală asupra proceselor implicate în cracking-ul hash-urilor, identificând funcțiile principale și interacțiunile dintre acestea. Aceste diagrame au ajutat echipa să definească procesele cheie, cum ar fi verificarea hash-urilor, identificarea tipului de hash, executarea algoritmilor brute-force și generarea rapoartelor.

Diagramele IDEF1x au fost esențiale în proiectarea structurii de date a aplicației. Ele au permis definirea entităților, atributelor și relațiilor dintre acestea, contribuind la gestionarea eficientă a datelor utilizate în procesul de cracking, inclusiv informații despre tipurile de hash-uri, wordlist-uri și rezultatele operațiilor.

Diagramele fluxului de date au oferit o viziune detaliată asupra modului în care datele circulă în aplicație. Ele au facilitat identificarea fluxurilor de date între diferitele module ale sistemului, cum ar fi introducerea hash-ului, procesarea algoritmilor brute-force și generarea rapoartelor pentru utilizatori.

În ansamblu, aceste diagrame au contribuit la dezvoltarea unei aplicații eficiente, coezive și ușor de utilizat pentru cracking-ul hash-urilor. Ele au fost esențiale pentru alinierea echipelor de dezvoltare și pentru luarea deciziilor informate legate de optimizarea proceselor și gestionarea datelor în cadrul aplicației.

Prin intermediul acestor diagrame, proiectul de dezvoltare a aplicației pentru cracking-ul hash-urilor a obținut o bază solidă pentru a asigura calitatea și eficiența soluției oferite. Diagramele au fost instrumente valoroase în acest proces și au contribuit la succesul proiectului.