**PROPUNERE DE PROIECT**

**Departamentul:** *Ingineria Software și Automatică*

**Programul de studii : Securitatea Informationala**

**Nume, prenume student: Chirita Stanislav**

**Grupa academică: SI-211**

**Conducator: asist.univ. Masiutin Maxim**

|  |  |
| --- | --- |
| **Tema:** | **Sistem integrat pentru interceptarea și analiza traficului de rețea** |
| **Scopul:** | Dezvoltarea unui modul integrat într-o aplicație GUI care automatizează interceptarea și analiza traficului de rețea. Modulul va simplifica identificarea vulnerabilităților și comportamentelor suspecte, oferind unelte eficiente pentru monitorizarea rețelei în timp real și post-eveniment, într-un mod structurat și accesibil utilizatorilor. |
| **Obiective:** | * **Cercetarea soluțiilor existente**: Studierea instrumentelor consacrate precum Tshark și Wireshark pentru interceptarea și analiza traficului de rețea, identificând avantajele și limitările acestora. * **Definirea cerințelor sistemului**: Stabilirea specificațiilor tehnice în funcție de cerințele utilizatorilor, pentru a asigura ușurința de utilizare și eficiența în analiza datelor din trafic. * **Proiectarea arhitecturii modulului**: Integrarea capabilităților de captare și analiză a pachetelor de rețea într-un model unitar, care să permită utilizarea instrumentelor de bază (Tshark, Wireshark) prin intermediul unei interfețe grafice simplificate. * **Dezvoltarea unei baze de date**: Crearea unei structuri de date pentru organizarea și salvarea capturilor și analizelor efectuate asupra traficului, cu posibilitatea de a le accesa ulterior. * **Dezvoltarea interfeței grafice**: Crearea unei GUI intuitive, prin care utilizatorii să poată gestiona capturarea pachetelor, filtrarea, vizualizarea și analiza datelor, fără a necesita cunoștințe tehnice avansate. * **Automatizarea proceselor**: Implementarea unor mecanisme automate pentru interceptarea traficului, analiza și generarea de alerte pentru comportamente suspecte, reducând astfel timpul și efortul necesar monitorizării manuale. * **Implementarea algoritmilor de analiză**: Dezvoltarea unor algoritmi eficienți de analiză a pachetelor capturate, care să identifice anomalii sau atacuri, precum atacuri de tip Man-in-the-Middle (MitM), scanări de porturi, sau exfiltrări de date. |