MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___" _____ 2025

METODE ȘI TEHNOLOGII ÎN INGINERIA SOCIALĂ PENTRU ANALIZA VULNERABILITĂȚILOR

Proiect de master

Student: _____ **Marcu Artiom, SI-231M**

Coordonator: _____ **Putere Alexandru, lect. univ.**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2025

REZUMAT

Lucrarea oferă o analiză detaliată a ingineriei sociale, un domeniu esențial în securitatea informațională, care valorifică vulnerabilitățile umane pentru a compromite sisteme și informații. Se discută despre diversele metode de atac, cum ar fi phishing-ul, baiting-ul și pretextarea, evidențiind impactul emotiilor și comportamentului uman asupra succesului acestor atacuri. Importanța conștientizării utilizatorilor și a educației în prevenirea atacurilor de inginerie socială este de asemenea subliniată, demonstrând că intervențiile educaționale pot îmbunătăți semnificativ gradul de rezistență al angajaților.

Social Engineer Toolkit (SET) este prezentat ca un instrument cheie utilizat pentru simularea atacurilor de inginerie socială. Experimentările controlate descrise în lucrare au utilizat SET pentru a analiza reacțiile utilizatorilor la diverse tipuri de atacuri, ceea ce a permis identificarea vulnerabilităților critice, atât la nivel individual, cât și organizațional. Rezultatele experimentelor sugerează că politicile de securitate ineficiente și lipsa autentificării multi-factor contribuie semnificativ la succesul atacurilor, confirmând interdependența dintre vulnerabilitățile umane și cele tehnologice.

Lucrarea recomandă o abordare integrată a securității informaționale, care să includă atât măsuri tehnice, cât și politici organizaționale clare. Educația continuă a utilizatorilor, implementarea unor politici stricte privind accesul la date și utilizarea tehnologiilor avansate, cum ar fi autentificarea multi-factor, sunt prezentate ca fiind esențiale pentru reducerea riscurilor asociate atacurilor de inginerie socială. Cercetarea subliniază, de asemenea, provocările etice asociate utilizării ingenieriei sociale în teste și necesitatea reglementărilor clare în acest sens.

ABSTRACT

This project provides a detailed analysis of social engineering, a critical aspect of information security that exploits human vulnerabilities to compromise systems and sensitive data. It discusses various attack methods, including phishing, baiting, and pretexting, emphasizing the influence of emotions and human behavior on the success of these attacks. The importance of user awareness and education in preventing social engineering attacks is highlighted, demonstrating that educational interventions can significantly enhance employees' resilience.

The Social Engineer Toolkit (SET) is introduced as a key tool for simulating social engineering attacks. Controlled experiments described in the paper utilized SET to assess user reactions to different types of attacks, identifying critical vulnerabilities at both individual and organizational levels. The results suggest that ineffective security policies and the absence of multi-factor authentication significantly contribute to the success of such attacks, confirming the interdependence between human and technological vulnerabilities.

The paper advocates for an integrated approach to information security that incorporates both technical measures and clear organizational policies. Continuous user education, the implementation of strict data access policies, and the use of advanced technologies like multi-factor authentication are presented as essential for mitigating risks associated with social engineering attacks. Additionally, the research highlights ethical challenges related to the use of social engineering in testing and the necessity for clear regulations in this area.

CUPRINS

INTRODUCERE

Securitatea informațională reprezintă unul dintre cele mai dinamice și complexe domenii ale erei digitale, având un impact semnificativ asupra tuturor aspectelor vieții moderne. Cu fiecare avans tehnologic, apar noi provocări legate de protecția datelor și a sistemelor informatice, iar amenințările evoluează în mod constant pentru a exploata vulnerabilitățile existente. Printre acestea, ingineria socială s-a impus ca una dintre cele mai insidioase metode de atac, concentrându-se nu doar pe slăbiciunile tehnologice, ci mai ales pe cele umane. Această disciplină reprezintă o combinație de tehnologie și psihologie, utilizată de atacatori pentru a manipula comportamentele utilizatorilor și pentru a obține acces la informații sau resurse critice.

Această lucrare de cercetare pune accent pe relevanța ingineriei sociale în contextul securității informaționale, explorând metodele utilizate de atacatori, precum și tehnologiile disponibile pentru simularea și prevenirea acestor atacuri. Alegerea acestei teme este justificată de creșterea alarmantă a atacurilor bazate pe inginerie socială, precum phishing-ul, pretextarea și baiting-ul, care exploatează adesea neglijența sau lipsa de conștientizare a utilizatorilor. Conform studiilor recente, peste 85% dintre atacurile cibernetice implică o componentă de inginerie socială, subliniind necesitatea unor cercetări aprofundate și a dezvoltării unor soluții adecvate pentru contracararea acestora.

Un aspect unic al acestei lucrări este analiza detaliată a Social Engineer Toolkit (SET), unul dintre cele mai utilizate instrumente pentru simularea atacurilor de inginerie socială. SET oferă o platformă versatilă pentru crearea de scenarii controlate, permitând cercetătorilor să testeze reacțiile utilizatorilor și să identifice vulnerabilități critice într-un mediu sigur. Prin utilizarea acestui instrument în combinație cu alte tehnologii, precum Metasploit și BeEF, lucrarea își propune să ofere o perspectivă holistică asupra atacurilor de inginerie socială și a contramăsurilor posibile.

De asemenea, cercetarea subliniază rolul vulnerabilităților umane în cadrul securității informaționale. Factorul uman este adesea considerat cea mai slabă verigă în lanțul de securitate, iar atacurile de inginerie socială profită de lipsa de conștientizare, curiozitatea sau presiunea emoțională a utilizatorilor. Lucrarea explorează metodele prin care aceste vulnerabilități pot fi reduse, inclusiv prin educația continuă a utilizatorilor, implementarea unor politici stricte de securitate și utilizarea tehnologiilor avansate, cum ar fi autentificarea multi-factor.

Importanța acestui subiect depășește granițele teoretice, având implicații practice semnificative pentru mediul organizațional și personal. De exemplu, sectorul financiar, cel medical sau cel educațional sunt doar câteva dintre domeniile care se confruntă cu riscuri crescânde datorită atacurilor de inginerie socială. Această cercetare nu doar că analizează metodele utilizate de atacatori, dar propune și soluții concrete pentru prevenirea și gestionarea acestor amenințări. Educația utilizatorilor și dezvoltarea unei culturi de securitate în organizații reprezintă pilonii principali ai strategiei propuse.

Totodată, lucrarea adresează și implicațiile etice ale utilizării ingineriei sociale, subliniind necesitatea unui cadru de reglementare clar pentru testarea și aplicarea acestor metode. Deși ingineria socială poate fi folosită în scopuri benefice, cum ar fi testarea securității și creșterea gradului de conștientizare, utilizarea necorespunzătoare poate avea consecințe grave asupra confidențialității și siguranței utilizatorilor.

Astfel, această lucrare de cercetare împreună analiza teoretică și evaluarea practică pentru a oferi o perspectivă completă asupra ingineriei sociale. Obiectivul principal este de a contribui la dezvoltarea unor soluții eficiente și etice pentru prevenirea atacurilor, consolidând astfel securitatea informațională într-un mediu din ce în ce mai complex și provocator.

BIBLIOGRAFIE

[1] "2024 Data Breach Investigations Report," Verizon Business. Accessed: Jan. 13, 2025. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[2] "Cost of a data breach 2024 | IBM." Accessed: Jan. 13, 2025. [Online]. Available: https://www.ibm.com/reports/data-breach

[3] "Cybersecurity Framework," *NIST*, Nov. 2013, Accessed: Jan. 13, 2025. [Online]. Available: https://www.nist.gov/cyberframework

[4] "DNSC." Accessed: Jan. 13, 2025. [Online]. Available: https://dnsc.ro/

[5] "OWASP Top Ten | OWASP Foundation." Accessed: Jan. 13, 2025. [Online]. Available: https://owasp.org/www-project-top-ten/

[6] "Publications | ENISA." Accessed: Jan. 13, 2025. [Online]. Available: https://www.enisa.europa.eu/publications

[7] "Resources & Tools | CISA." Accessed: Jan. 13, 2025. [Online]. Available: https://www.cisa.gov/resources-tools

[8] "Symantec Enterprise Blogs." Accessed: Jan. 13, 2025. [Online]. Available: https://www.security.com/

[9] K. D. Mitnick, "THE ART OF DECEPTION".

[10] "What is Social Engineering? | Definition," /. Accessed: Jan. 13, 2025. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering