MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Inginerie Software și Automatică

Admis la susținere
Șef departament:
Fiodorov Ion, conf. univ., dr.

_____
„ ____”_____ 2022

Analiza comparativă a soluțiilor de identificare a vulnerabilităților

Teză de master

Student: **Palai Ina, SI-211M**

Conducător: **Bulai Rodica, asist. univ.**

Chișinău, 2023

ADNOTARE

Prezenta teză reflectă analiza și evaluarea soluțiilor de identificare a vulnerabilităților din perspectiva preciziei, fiabilității, scalabilității și raportării. Această cercetare se concentrează pe analiza utilizării diferitor scanere de vulnerabilități și pe metodologia aferentă acestora pentru a detecta vulnerabilități și încearcă să identifice noi mecanisme care pot fi implementate pentru a securiza activele informaționale.

Lucrarea reprezintă un studiu asupra funcționalităților mai multor scanere, fiind analizate totodată și tendințele de dezvoltare. Aceasta include descrierea unor concepte fundamentale privind procesul de identificare a vulnerabilităților, descrierea celor mai utilizate soluții la momentul actual și compararea acestora din punct de vedere a funcționalităților oferite, performanței rezultatelor și contribuirea la evaluarea de risc.

Analiza realizată oferă o privire generală asupra multitudinii de instrumente de scanare a vulnerabilităților, fiecare oferind o combinație unică de capabilități în dependență de testele integrate.

ANNOTATION

This thesis reflects the analysis and evaluation of vulnerability identification solutions from the perspective of accuracy, reliability, scalability and reporting. This research focuses on analyzing the use of different vulnerability scanners and their related methodology to detect vulnerabilities and tries to identify new mechanisms that can be implemented to secure information assets.

The work represents a study on the functionalities of several scanners, the development trends being analyzed at the same time. This includes the description of some fundamental concepts regarding the vulnerability identification process, the description of the most used solutions at the moment and their comparison in terms of the functionalities offered, the performance of the results and the contribution to the risk assessment.

The analysis provides an overview of the multitude of vulnerability scanning tools, each offering a unique combination of capabilities depending on the integrated tests.

CUPRINS

INTRODUCERE

Securitatea cibernetică este o problemă pentru companiile de toate dimensiunile. Având în vedere că companiile fac tranzacții într-o lume bazată pe aplicații, majoritatea organizațiilor sunt dependente tehnologic. Indiferent de dimensiunea și maturitatea infrastructurii informaționale a organizației, aproape toate activele sunt expuse la riscuri cu diferite tipuri de amenințări, aceasta constituind suprafața de atac, măsurarea căreia este importantă înainte de a acționa asupra reducerii riscurilor care afectează aceste active.

O mare parte din atacurile de securitate rezultă din configurări greșite și vulnerabilități cunoscute, iar înțelegerea modului de efectuare și utilizare a scanărilor de vulnerabilități poate oferi un nivel important de protecție. Cu o multitudine de vulnerabilități legate de sistemele de operare, rețele și aplicații, companiile realizează din ce în ce mai mult nevoia de a evalua și de a gestiona riscurile de securitate. Acest lucru necesită o abordare eficientă pentru a proteja întreprinderile, ceea ce presupune și scanarea vulnerabilităților cu instrumente adecvate, care pot arăta unde se află vulnerabilitățile și oferă suport pentru remedierea acestora. Infractorii cibernetici folosesc adesea instrumente automate pentru a găsi și exploata vulnerabilitățile cunoscute. Ei scanează infrastructura informațională pentru a obține metodă de intrare și pentru a executa comenzi neautorizate. Companiile pot folosi aceleași instrumente de scanare pentru a identifica și urmări vulnerabilitățile cunoscute, astfel încât să le remedieze înainte ca infractorii să le exploateze. În acest fel, va fi asigurat că compania este întotdeauna conștientă de defectele infrastructurii informaționale și că le poate corecta înainte de a putea fi exploatate.

Amenințările variază de la organizație la organizație și de la activele implicate. O strategie de securitate cibernetică care face față amenințărilor unei organizații trebuie să fie contextuală. Procesul de scanare a vulnerabilităților ajută companiile să se asigure că sunt în fruntea gestionării activelor, zonelor slabe din perspectiva de securitate. Instrumentele de scanare a vulnerabilităților adaugă contribuții la programul mai larg de gestionare a riscurilor, evidențiind unde se află riscurile cele mai grave și contribuind la planurile de remediere a riscurilor.

În prezent, există un număr mare de soluții de scanare disponibile, însă acestea diferă după rata de detectare, rata de falsuri pozitive, timpul de scanare și mulți alți factori, care necesită a fi evaluați. Alegereasoluției de identificare a vulnerabilităților optime în dependență de resursele deținute reprezintă etapă importantă din cadrul strategiei de securitate cibernetică, ce contribuie la identificarea posibilelor puncte slabe de securitate, și ulterior la definirea nivelului riscurilor de securitate. Acestea permit organizațiilor să-și monitorizeze în mod consecvent și holistic activele, și să ia măsuri de remediere/corecție înainte cacareva abateri să devină perturbatoare.

BIBLIOGRAFIE

1. Iskander Zulkarneev, Andrey Kozlov, New Approaches of Multi-agent Vulnerability Scanning Process – IEEE, 2021
2. Sam Humphries, 4 Stages of Vulnerability Management: A Process for Risk Mitigation – Exabeam, 2022, [citat 07.09.2022]. Disponibil: https://www.exabeam.com/information-security/vulnerability-management/
3. Brian Drake, Exploring the Origins and Evolution of Vulnerability Management – Igicybersecurity, 2020, [citat 09.09.2022]. Disponibil: https://blog.igicybersecurity.com/origins-and-evolution-of-vulnerability-management
4. Vulnerability assessment – Schaumburg: ISACA, 2017
5. A. Subhangani, B. Anita Chaudhary, Vulnerability Scanning – TechRxiv, 2022
6. Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică, [citat 12.09.2022]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro
7. Sowmyashree A., Dr. H. S. Guruprasad, Evaluation and Analysis of Vulnerability Scanners: Nessus and OpenVAS - International Research Journal of Engineering and Technology, 2020
8. Stephen Cooper, Nessus Vulnerability Scanner Review – Comparitech, 2022
9. Nessus 8.14.x User Guide – Tenable, 2022
10. Jan-Oliver Wagner, Michael Wiegand, Tim Brown, Carsten Koch Mauthe, OpenVAS Compendium - Intevation GmbH, 2009
11. OpenVAS, Reporting Documentation Release 1.4.4 – TheGroundZero, 2022
12. Nexpose, Deployment & MVM Migration Utility Guide Product version: 6.0 – Rapid7, 2015
13. Abheenesh Kejiou, Girish Bekaroo, A Review and Comparative Analysis of Vulnerability Scanning Tools for Wireless LANs – IEEE, 2022
14. Qualys Vulnerability Scanner – Bugcrowd, [citat 26.09.2022]. Disponibil: https://www.bugcrowd.com/glossary/qualys-vulnerability-scanner/
15. Sunny Wear, Burp Suite Cookbook: Practical Recipes to Help You Master Web Penetration Testing with Burp Suite – Packt, 2018
16. Sagar Rahalkar, A Complete Guide to Burp Suite – Apress, 2021
17. Acunetix, v12 Product Manual - Acunetix Ltd, 2018
18. Rajkumar, Invicti Web Application Security Scanner Review – Softwaretestingmaterial, 2022, [citat 04.10.2022]. Disponibil: https://www.softwaretestingmaterial.com/invicti-web-application-security-scanner/

19. Karen Scarfone, IBM Security QRadar: SIEM product overview - Scarfone Cybersecurity, 2015, [citat 07.10.2022]. Disponibil: https://www.techtarget.com/searchsecurity/feature/IBM-Security-QRadar-SIEM-product-overview
20. IBM QRadar Tutorial – Mindmajix, 2022, [citat 07.09.2022]. Disponibil: https://mindmajix.com/ibm-qradar-tutorial
21. Comparing Vulnerability Scanner Software Products, Capterra, 2022, [citat 10.11.2022]. Disponibil: https://www.capterra.com/vulnerability-scanner-software/
22. Best Vulnerability Scanner Software, g2, 2022, [citat 11.11.2022]. Disponibil: https://www.g2.com/categories/vulnerability-scanner
23. Yuji Ogawa, Tomotaka Kimura, Jun Cheng, Vulnerability Assessment for Machine Learning Based Network Anomaly Detection System - IEEE, 2020