Ministerul Educaţiei, Culturii și Cercetării
Universitatea Tehnică a Moldovei

Faculatea Calculatoare, informatică și microelectronică
Departamentul Ingineria Software și Automatică

RAPORT

Lucrare de Laborator nr.2
Disciplina: Proiectarea sistemelor informaționale
Tema :

A efectuat: Chirita Stanislav
A verificat: Magdei Octavian

Chişinău 2024

Introducere

Pe fondul creșterii continue a amenințărilor cibernetice, organizațiile moderne se confruntă cu necesitatea de a adopta soluții avansate pentru interceptarea, analiza și gestionarea traficului de rețea. În acest context, un sistem integrat pentru interceptarea și analiza traficului de rețea devine un element critic pentru asigurarea unui management proactiv al riscurilor și securității rețelelor. Acest sistem permite colectarea, analiza și corelarea datelor din trafic pentru identificarea amenințărilor, răspunsul rapid la incidente și reducerea riscurilor asociate.

Obiectivul principal al proiectului constă în colectarea cerințelor funcționale și nefuncționale necesare pentru integrarea și operarea acestui sistem, precum și identificarea specificațiilor tehnice, a constrângerilor și a riscurilor asociate.

Pentru a atinge acest obiectiv, este necesară analiza și documentarea atentă a cerințelor prin:

- Vizitarea mai multor organizații și intervievarea persoanelor-cheie, precum administratori de sistem și experți în securitate cibernetică.
- Observarea modului în care astfel de soluții sunt implementate și utilizate în medii reale, obținând astfel o perspectivă detaliată asupra abordărilor și provocărilor întâmpinate.

Această cercetare va include:

- **Cerințele funcționale și nefuncționale** ale sistemului, care descriu funcționalitățile esențiale și atributele de performanță sau calitate necesare.
- **Specificațiile tehnice**, care oferă o descriere detaliată a componentelor și resurselor implicate.
- **Planul de testare**, care subliniază metodele utilizate pentru a verifica performanța și eficacitatea sistemului implementat.
- **Constrângerile tehnice și organizaționale**, care pot influența integrarea și operarea acestuia.
- **Riscurile asociate**, care trebuie gestionate pentru a asigura succesul implementării și funcționării continue.

Această lucrare își propune să contribuie la o mai bună înțelegere a proceselor implicate în proiectarea și implementarea unui sistem integrat pentru interceptarea și analiza traficului de rețea, oferind informații relevante despre bunele practici și cerințele critice pentru asigurarea unui management eficient al securității rețelelor.

Cerințe Funcționale

Cerințele funcționale definesc acțiunile și funcționalitățile specifice pe care sistemul integrat pentru interceptarea și analiza traficului de rețea trebuie să le îndeplinească pentru a răspunde cerințelor organizației. Aceste cerințe stabilesc modul de operare al sistemului, interacțiunea utilizatorilor cu acesta și rezultatele așteptate.

Colectarea și corelarea datelor:

- Colectarea datelor din trafic: Sistemul trebuie să intercepteze și să colecteze datele din rețea, inclusiv pachetele de trafic, logurile și fluxurile de rețea de la diverse surse (servere, stații de lucru, firewall-uri, switch-uri).
- Corelarea informațiilor colectate: Sistemul trebuie să analizeze și să coreleze datele pentru a identifica modele sau comportamente anormale indicative ale unor potențiale amenințări.

Detectarea și răspunsul la amenințări:

- Detectarea activităților suspecte: Sistemul trebuie să monitorizeze traficul în timp real pentru a identifica semnături sau comportamente care indică atacuri sau intruziuni.
- Alertare în timp real: Generarea automată a alertelor în cazul identificării unor amenințări critice, specificând natura, sursa și impactul potențial.

Managementul și analiza datelor:

- Interfață centralizată de management: Oferirea unei interfețe grafice intuitive pentru vizualizarea și gestionarea datelor de securitate.
- Funcționalități de căutare și filtrare: Permisiunea de a căuta evenimente după criterii specifice (timp, adresă IP, tipul incidentului).
- Generarea de rapoarte personalizabile: Crearea de rapoarte care reflectă activitatea sistemului, incidentele și analizele detaliate ale traficului.

Integrarea cu alte sisteme:

- Compatibilitate multiplă: Suport pentru diverse tehnologii și dispozitive din rețea (firewall-uri, antivirusuri, platforme de monitorizare).
- Export și schimb de date: Funcționalități pentru integrarea cu alte soluții software, precum sisteme de ticketing sau platforme de automatizare.

Managementul utilizatorilor și accesului:

- Autentificare robustă: Suport pentru autentificare multifactorială (MFA) și implementarea unui mecanism de autentificare sigur.
- Controlul rolurilor și permisiunilor: Alocarea accesului diferențiat în funcție de roluri (administrator, analist, operator).

Funcționalități de personalizare:

- Personalizarea alertelor: Configurarea pragurilor și regulilor pentru alertele generate.

Cerințe Nefuncționale

Cerințele nefuncționale stabilesc atributele de calitate ale unui sistem integrat pentru interceptarea și analiza traficului de rețea. Aceste cerințe nu descriu ce face sistemul, ci cum trebuie să își îndeplinească funcționalitățile definite, asigurând performanță, securitate și fiabilitate optime.

Performanță:

- **Timp de răspuns**: Sistemul trebuie să proceseze evenimentele și să genereze alerte critice în mai puțin de 5 secunde de la detectarea unui eveniment de securitate.
- **Eficiența utilizării resurselor**: Sistemul trebuie să funcționeze fluent pe servere cu resurse medii, utilizând sub 70% din capacitatea CPU și RAM în condiții de sarcină maximă.
- **Scalabilitate**: Sistemul trebuie să gestioneze cel puțin 1 milion de evenimente pe secundă (EPS) fără degradarea performanței, cu posibilitatea de extindere pentru volume mai mari de date.

Securitate:

- **Protecția datelor**: Datele colectate și stocate trebuie criptate folosind standarde avansate, precum AES-256, atât în tranzit (SSL/TLS), cât și în repaus.
- **Autorizare și autentificare**: Implementarea autentificării multifactoriale (MFA) și utilizarea unui model bazat pe roluri (RBAC) pentru a limita accesul la funcționalitățile relevante.
- **Rezistență la atacuri**: Protecția împotriva atacurilor cibernetice, inclusiv atacuri de tip DoS, exploatări de vulnerabilități și acces neautorizat.

Fiabilitate și disponibilitate:

- **Disponibilitate**: Sistemul trebuie să asigure o disponibilitate de 99.99%, funcționând continuu în toate scenariile operaționale.
- **Backup și recuperare**: Implementarea de mecanisme automate de backup periodic și funcționalități de recuperare rapidă în caz de defecțiuni hardware sau pierderi de date.
- **Toleranță la erori**: Sistemul trebuie să includă redundanță la nivel de hardware și software pentru a preveni întreruperile cauzate de erori tehnice.

Compatibilitate:

- **Integrare multiplatformă**: Compatibilitatea cu echipamentele și aplicațiile de securitate moderne (firewall-uri, soluții antivirus, platforme de gestionare a incidentelor).
- **Interoperabilitate**: Suport pentru standarde deschise (ex.: syslog, SNMP, API-uri REST) pentru integrarea cu alte sisteme și fluxuri de lucru existente.

Ușurință în utilizare:

- **Interfață intuitivă**: O interfață simplă, ușor de navigat, cu opțiuni de personalizare pentru afișarea datelor relevante fiecărui utilizator.
- **Ghiduri și suport**: Documentație completă, tutoriale interactive și suport tehnic, asigurând o curba de învățare minimă pentru utilizatori.

Scalabilitate și extensibilitate:

- **Adăugarea surselor noi de date**: Sistemul trebuie să permită integrarea rapidă a noilor surse de evenimente fără modificări majore în configurație.
- **Extensibilitate modulară**: Sistemul trebuie să suporte adăugarea de noi funcționalități prin module adiționale, fără a afecta performanța generală.

Specificațiile Tehnice

Specificațiile tehnice definesc arhitectura, tehnologiile și structura sistemului integrat pentru interceptarea și analiza traficului de rețea, adaptat pentru o aplicație Windows cu interfață grafică. Sistemul include două baze de date: una pentru gestionarea utilizatorilor și alta pentru stocarea rezultatelor programului. Specificațiile se concentrează pe modul în care aceste componente interacționează pentru a colecta, analiza și gestiona datele.

Arhitectura Sistemului

Arhitectura aplicației este structurată în trei componente principale:

1. **Frontend (UI/UX)**:
    - Funcționalități:
        - Autentificarea și autorizarea utilizatorilor.
        - Vizualizarea rezultatelor programului într-un format grafic.
        - Gestionarea utilizatorilor și setările aplicației.
        - Afișarea alertelor și rapoartelor personalizate.
2. **Backend (Logica aplicației)**:
    - Implementat în limbaje precum **Python** pentru compatibilitate cu Windows.
    - Funcționalități:
        - Procesarea datelor introduse de utilizatori și stocate în bazele de date.
        - Generarea rapoartelor și analizelor în timp real.
        - Gestionarea operațiunilor CRUD (Create, Read, Update, Delete) pentru utilizatori și rezultate.
3. **Baza de Date**:
    - Sistemul utilizează două baze de date relaționale, implementate în **SQL Server** sau **SQLite** pentru aplicații locale:
        - **Baza de date pentru utilizatori**:
            - Structura tabelelor: ID utilizator, nume, email, roluri, parola hashată.
            - Funcționalități: autentificare, gestionarea permisiunilor, jurnalizare acces.
        - **Baza de date pentru rezultate**:
            - Structura tabelelor: ID rezultat, tip rezultat, data generării, valori analizate.
            - Funcționalități: stocare date brute și procesate, acces rapid la analize.

Concluzie: Lucrarea de laborator a demonstrat importanța utilizării unui model integrat pentru interceptarea și analiza traficului de rețea, subliniind pașii esențiali în proiectarea și implementarea unui astfel de sistem. Am realizat o abordare practică pentru definirea cerințelor funcționale și nefuncționale, precum și pentru dezvoltarea specificațiilor tehnice.

Implementarea unei arhitecturi bine definite, cu accent pe interfața grafică, logica aplicației și gestionarea bazelor de date, permite crearea unui sistem eficient, scalabil și sigur. Prin documentarea și aplicarea principiilor de design și integrare, sistemul proiectat oferă un suport semnificativ pentru managementul riscurilor și răspunsul rapid la incidentele de securitate.

Această lucrare contribuie la înțelegerea proceselor implicate în dezvoltarea unui sistem IT avansat, oferind un exemplu de bune practici și un cadru solid pentru dezvoltări viitoare. Rezultatele obținute reflectă o combinație echilibrată între cerințele teoretice și aplicabilitatea practică a soluției.