Universitatea Tehnică a Moldovei

Analiza şi monitorizarea atacurilor externe de penetrare a reţelei intranet a Poliţiei de Frontieră

Masterand:
Alexandru IANIŢCHI

Conducător:
lect. univ. Valeriu CERNEI

Chişinău – 2020

Ministerul Educaţiei Culturii şi Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

FACULTATEA Calculatoare, Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susţinere

Şef departament: conf. univ., dr. în informatică

Ion FIODOROV

„20" decembrie 2019

Analiza şi monitorizarea atacurilor externe de penetrare a reţelei intranet a Poliţiei de Frontieră

Teză de master în

Securitate informaţională

Masterand:

Alexandru IANIŢCHI (_____)

Conducător: lect. univ. Valeriu CERNEI (_____)

Chişinău – 2020

ADNOTAREA

Titlul: Analiza şi monitorizarea atacurilor externe de penetrare a rețelei intranet a Poliției de Frontieră

Masterand: Alexandru IANIŢCHI,

Lucrarea conţine un capitol ce descrie în linii generale activitatea Poliţiei de Frontieră, un capitol de introducere în tematica selectată, 4 capitole ce descriu activităţile implementate asupra temei, concluzie despre rezultatelor obţinute, bibliografie din 17 surse, 44 pagini de text de bază, 15 figuri, şi 2 anexe 11 pagini.

Cuvinte-cheie: analiză, monitorizare, atac, router, paravan de protecţie, IP, RouterOS, intranet, sisteme informatice, SIEM, vulnerabilităţi.

Scopul acestei lucrări este studiul celor mai frecvente tipuri de atacuri cibernetice asupra reţelei ”intranet” a Poliţiei de Frontieră, precum şi tehnicile utilizate pentru analiza şi monitorizarea acestor atacuri cibernetice.

Obiectivul de bază al acestei lucrări este de a securiza reţeaua informaţională ”intranet” a Poliției de Frontieră, prin utilizarea sistemelor software şi hardware care au ca scop colectarea, monitorizarea analizarea, blocarea şi raportarea atacurilor cibernetice de penetrare, precum şi studiul celor mai frecvente atacuri.

Metodologia aplicată în această lucrare este următoarea: studiu despre tipurile de atacuri cibernetice, studiu privind analiza şi monitorizarea atacurilor cibernetice utilizând dispozitive de gestionare a reţelelor cu paravan de protecţie, studiu privind tehnicile de dezvoltare a aplicaţiilor de colectare, monitorizare şi analiză atacuri cibernetice, implementare acestor studii.

Originalitatea acestei lucrări constă în dezvoltarea sistemului informaţional ”**Monitorizare şi analiză atac cibernetic extern**” care are ca scop colectarea, monitorizarea şi analiza atacurilor cibernetice de penetrare a reţelei ”intranet” a Poliţiei de Frontieră.

Dezvoltarea versiunii curente a sistemului informaţional a fost realizată de către masteranzii Dumitru Tintiuc şi Alexandru Ianiţchi.

Din analiza datelor acumulate/monitorizate prin intermediul sistemelor informatice dezvoltate (descrise în lucrare), s-a constat faptul că ameninţările de natură informatică asupra reţelei ”intranet” a Poliţiei de Frontieră sunt într-un număr foarte mare şi sunt de diverse tipuri. Totodată, s-a conştientizat faptul despre importanţa menţinerii la un nivel înalt a securităţii informaţiei prin alocarea resurselor financiare cu scop de achiziţionare a componentelor software şi hardware necesare blocării şi prevenirii atacurilor cibernetice, precum şi a formării şi menţinerii competentelor şi calificărilor necesare la nivelul resurselor de personal pentru securitatea informaţiei.

ANNOTATION

Title: Analysis and monitoring of cyberattacks on network ’intranet’ of the Border Police of the Republic of Moldova.

Magister: Alexandru Ianiţchi

The thesis contains a chapter describing in general general lines the Border Police, an introductory chapter on selected topics, 4 chapters describing implementation activities on the theme, conclusion on the obtained results, bibliography from 17 sources, 44 pages of basic text, 15 figures, and 2 annexes 11 pages

Key-words: monitoring, blocking, attack, router, firewall, IP, RouterOS, intranet, computer systems, SysLog, SIEM.

The main goal of this thesis is to study the most frecvent cyberattacks on network ’intranet’ of the Border Police, as well the techniques used in order to monitor and analyse theses cyberattacks.

The main objective of the research is to provide security to computer system/network ’intranet’ of the Border Police using software and hardware systems. Due to theses systems we store, monitor, analyse, and prevent all the cyberattacks.

Our approaches concern several studies: types of cyberattacks, measures to block and prevent the cyberattacks, techniques of developing of data storage, the implementation of theses studies.

The originality of this work consists in the development of the informational system "Monitoring and analysis of external cyber attack" which aims to collect, monitor and analyze cyber attacks penetrating the "intranet" network of the Border Police.

The current version of IS belongs to Dumitru Tintiuc, and the analysis of data storage belongs to Alexandru Ianitchi.

From the analysis of the data accumulated / monitored through the developed computer systems (described in the paper), it was found that the threats of computer nature on the "intranet" network of the Border Police are in a very large number and are of different types. At the same time, it was made aware of the importance of maintaining a high level of information security by allocating the financial resources for the purpose of acquiring the software and hardware components necessary to block and prevent cyber attacks, as well as the training and maintenance of the necessary skills and qualifications at the level of personnel resources. for information security.

CUPRINS

INTRODUCERE

Odată cu finalizarea cursurilor teoretice de masterat studiate pe parcursul anului de învățământ 2018-2019 am decis ca scop să îmbunătățim sistemul de securitate a rețelei ”intranet” a Poliției de Frontieră cu noi funcționalități de analiză şi monitorizare a atacurilor cibernetice de penetrare.

Sarcinile acestei lucrări sunt:

- studiu privind tipurile de atacuri frecvente întâlnite de penetrare a dispozitivelor de gestionare a rețelelor informaționale cu paravan de protecție (în continuare - router);
- studiu privind implementarea măsurilor de securitate în router-ele de model MikroTik;
- elaborarea unui sistem informațional de tip SIEM (Managementul Evenimentelor și al Securitatii Informatiilor; eng: Security information and event management) cu funcționalitate de interacțiune cu sistemul de operare RouterOS, precum și studierea sistemelor actuale de acest tip;
- prezentarea rezultatelor obținute în urma analizei şi monitorizării datelor de către sistemul informațional dezvoltat.

Rețeaua informațională intranet a Poliției de Frontieră constă din 2 subrețele, și anume:

1. Rețea TETRA, rețea internă formată pe baza unui sistem modern de telecomunicații aplasată pe sectorul frontierei de stat. Sistemul de telecomunicații este bazat pe transmisia de date între stațiile de bază ale rețelelor de radiorelee cu transmisie digitală de date prin intermediul comunicațiilor radio pe distanțe scurte și medii. Acest lucru face posibilă schimbul de date în mod on-line între subdiviziunile instituției. Pentru transmiterea de date, video și voce este utilizat standardul TETRA cu frecvențe Micro-Wave. În rețeaua dată accesul la resursele internet este blocat.
2. Rețea ”intranet” (figura), rețea internă cu zonă demilitarizată și cu acces la următoarele resurse informaționale:
   - Resurse Internet. Furnizori de Internet în sediul central și subdiviziunile Poliției de Frontieră amplasate în municipiul Chișinău: Serviciul Tehnologia Informației și Securitate Cibernetică, din subordonarea Guvernului Republicii Moldova (STISC) – IP public static; Î.S. ”MoldTelcom” – IP public static; S.A. ”Orange” – IP public static. Subdiviziunile Poliției de Frontieră amplasate în raionale Republicii Moldova: Î.S. ”MoldTelcom” – IP public static; S.A. ”Orange” – IP public dinamic.
   - Rețelele\subrețele interne ale subdiviziunilor Poliției de Frontieră (Direcții Regionale, Sectoare, Puncte de trecere a frontierei de stat). Modul de accesare a acestora:
     - în baza contractelor de prestare a serviciilor de telecomunicații, subdiviziunile

Poliției de Frontieră sunt asigurate cu acces la resursele Internet și IP public static/dinamic;

- dotarea subdiviziunilor cu dispozitive de gestionare a rețelelor cu paravan de protecție (router de tip MikroTik);
- crearea canalelor securizate prin tehnologia VPN utilizând protocolul L2TP cu IPsec dintre router-ul central al Inspectoratului General al Poliției de Frontieră și router-ele din subdiviziuni;

- Rețeaua guvernamentală a Republicii Moldova, gestionată de către Serviciul Tehnologia Informației și Securitate Cibernetică.

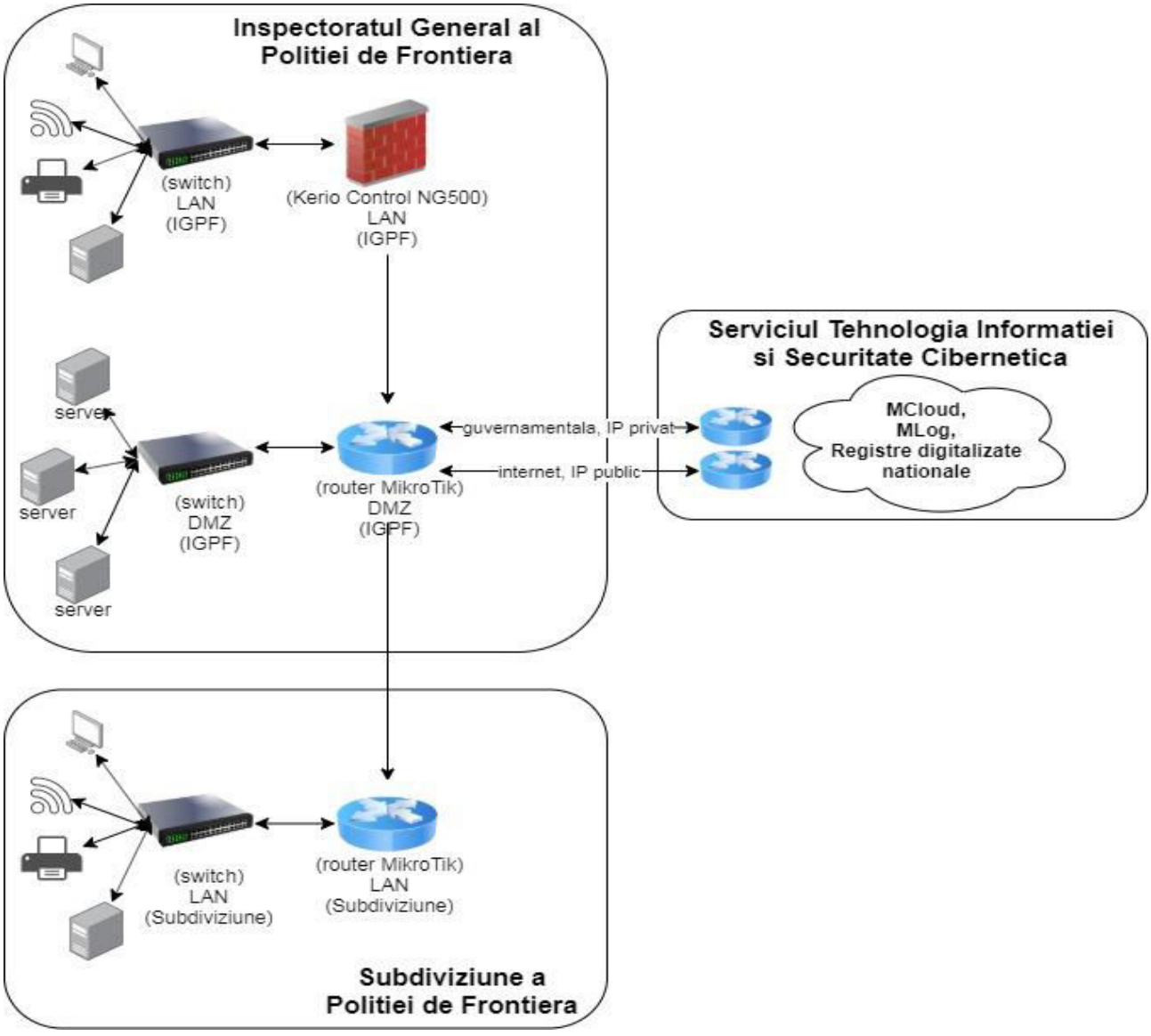

Figura. Structura generală a rețelei ”intranet” (www.draw.io)

Iniţial, au fost depistate următoarele carenţe :

- lipsa regulilor de jurnalizare a atacurilor de penetrare asupra router-elor cu paravan de protecție din gestiunea Poliției de Frontieră;

- reguli minime de filtrare/blocare a atacurilor de penetrare aplicate pe router-ele cu paravan de protecție din gestiunea Poliției de Frontieră;
- în multe subdiviziuni lipseau router-e cu paravan de protecție în subdiviziunile Poliției de Frontieră.

Examinând starea inițială și conștientizând faptul că activitatea de control și supraveghere a frontierei de stat este dependent de domeniul tehnologiilor informaţionale, sistemul de securitate a rețelei ”intranet” necesită a fi apt să prevină sau să blocheze diverse atacuri cibernetice, înainte de a se produce incidentele de scurgere\modificare\acces neautorizate de\la date.

CONCLUZIE

Obiectivul urmărit prin prezenta lucrare a fost atins prin desfășurarea unor mai multor acțiuni, și anume:

1. Studiul tipurilor de atacuri de penetrare frecvente întâlnite a dispozitivelor de gestiune a rețelelor informaționale cu paravan de protecție:

   Am stabilit că există diverse tipuri de atacuri cibernetice de penetrare și este o necesitate stringentă de a implementa măsuri de stopare și prevenire a acestora. Totodată, aceste măsuri de securizare trebuie să fie implementate în complex cu toate măsurile descrise în Sistemul de Management al Securității Informației.

2. Implementarea măsurilor de securitate în router-ele de model MikroTik:

   În primul rând pentru a aplica reguli pe paravanele de protecție este necesar de a cunoaște cel puțin la nivel mediu următoarele domenii: rețelele de calculatoare, nivelurile și protocoalele de comunicație, precum și serviciul ”iptable”. În cazul când doar se folosesc reguli pentru paravanul de protecție identificate (găsite) prin diferite surse oficiale/neoficiale din Internet fără a intra în esența regulii, atunci există riscul de blocare completă a unor servicii de rețea acceptate sau ceva mult mai grav, ca exemplu: încercările de penetrare să nu fie depistate și blocate.

   În lucrarea dată au foast consultate surse oficiale din Internet (wiki.mikrotik.com, mikrotik.com, blog.mikrotik.com, site-uri oficiale ale companiilor ce oferă cursuri de administrare RouterOS) pentru a identifica acelea reguli care ar aduce un rezultat la depistarea și blocarea atacurilor cibernetice de penetrare. Totodată, menţionăm că unele reguli privind jurnalizarea IP-urilor publice de la care se încearcă ”scanarea” porturilor de rețea, aplicate în luna iulie 2019, nu au ”reacționat” (primire 0 pachete), ce semnifică că atacuri de acest gen nu au fost întreprinse asupra router-elor sau IP-urile publice au fost blocate de regulile de mai sus. Totuși, nu este binevenit să fie dezactivate aceste reguli din motiv că analizând parametrii regulilor aplicate, observăm că scopul acestor reguli sunt de a preveni atacurile complexe, și bine gândite.

   În aceeaşi ordine de idei, necesită a fi verificate cu regularitate și la versiunile sistemului RouterOS, deoarece conform știrilor de pe site-ul www.cvedetails.com sunt multe vulnerabilități depistate la versiunile vechi și numai prin înnoirea sistemului pot fi înlăturate aceste carenţe.

3. Dezvoltarea unui sistem informațional de tip SIEM cu funcționalitate de interacțiune cu sistemul de operare RouterOS, precum și studierea sistemelor actuale de acest tip:

Soluțiile SIEM menţionate în lucrare. asigura răspunsul la cele doua mari provocări și cerințe ale unei infrastructuri IT: administrarea securității IT și monitorizarea conformității cu reglementările actuale. Acest lucru are loc prin: vizualizare și control; detectarea și soluţionarea rapidă a incidentelor și încălcărilor de politici, evaluarea continuă a securității și conformității; audit eficient; îndeplinirea și monitorizarea conformității cu politicile interne. Totodată, luând în considerație complexitatea acestor sisteme, costul mare, precum și sarcinile acestei lucrări, am decis dezvoltarea unui sistem informațional care ar procesa date de la sistemul RouterOS, cât și interacțiune cu acesta.

Versiunea curentă a sistemului informațional ”Monitorizare și analiză atac cibernetic extern” (SI ”MAACE”) permite salvarea și monitorizarea în timp real a datelor care sunt generate de regulile setate în router-ele din gestiunea Poliției de Frontieră. O funcționalitate importantă a acestui sistem este de a bloca automatizat în toate router-ele IP-urile publice de pe care s-au încercat cel puțin de 7 ori atacuri cibernetice de penetrare. Analiza și raportarea altor tipuri de acțiuni, cum ar fi:

- depistarea IP-urile publice de la care într-o perioadă de timp (1-2 zile) s-au încercat intens atacuri;
- depistarea IP-urilor publice care au fost raportate furnizorilor de internet și iarăși întreprind acțiuni de atacuri.

nu sunt realizate într-un mod automatizat, doar manual, prin utilizarea altor aplicații dezvoltate pentru acest scop care permit procesarea textului: extragerea IP-urilor și a porturilor, exportul într-o bază de date SGBD Firebird și exportul în fișier Excel. Deja utilizând instrumentele Excel/SGBD putem primi rezultatul dorit.

În versiunea următoare a SI ”MAACE” necesită să fie implementate următoarele funcționalități:

- înregistrarea datelor de interes într-o bază de date bine structurată;
- automatizarea proceselor de analiză și raportare;
- integrarea, prin intermediul funcțiilor API, cu diferite surse din Internet care ar oferi date despre IP-urile publice: locația, persoană fizică/juridică, existența în liste negre, alte;
- raportarea prin diferite instrumente: grafic, textual, avertizare prin SMS/Bot-Telegram;
- citirea unor ”acțiuni” (scripturi) din fișiere/tabel care necesită a fi îndeplinite;
- alte.

4. Prezentarea rezultatelor obținute în urma procesării și analizării datelor de către sistemul informațional dezvoltat:

Prin implementarea SI ”MAACE” în Poliția de Frontieră s-a observat multiplele atacuri cibernetice de penetrare asupra dispozitivelor de gestionarea a rețelelor informaționale, precum și rolul important al sistemelor SIEM. Fără a implementa un astfel de sistem într-o instituție cu o organigramă complexă (*subdiviziuni, rețele multe de tip LAN, multe intrări de Internet, etc*) ar fi dificil de a realiza în ansamblu o analiză, prevenire și raportare a atacurilor cibernetice de penetrare.

În urma analizării datelor s-a constat ”tipul” atacatorilor:

- calculatoare infectate cu diferiți viruși și probabilitate mare că operatorul nu cunoaște despre acest fapt

  analiza atacului:

  1. atacuri permanente de la IP-uri publice cu adresă poștală reală;
  2. la același port de rețea;
  3. în perioada de zi a zilei.

- atacuri de ”începător”, posibil student la cursul de securitate informațională

  analiza atacului:

  1. atacuri intenţionate la anumite porturi de rețea implicite;
  2. atacuri de la un IP public cu adresă poștală reală din străinătate;
  3. scanarea porturilor de rețea utilizând aplicația NMAP;
  4. peste o perioadă mică de timp (1 ore) atacurile se opresc;

- atacuri realizate de ”expert”

  analiza atacului:

  1. atacuri intenţionate la anumite porturi de rețea implicite;
  2. atacuri intenţionate concomitente de la IP-uri diferite, dar din aceiași subrețea și toate din Data Centru (Cloud);
  3. peste o perioadă mare de timp (1-2 zile) atacurile se opresc.

BIBLIOGRAFIE

1. http://lex.justice.md/md/378478/, accesat în data de 10.10.2019.
2. **Publicații ale Institutului Național de Cercetare în Informatică București**, Revista Română de Informatică şi Automatică, vol. 26, nr. 4, 2016;
3. https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/eID_nov2015.pdf, accesat în data de 11.10.2019;
4. **Ghid de bune practici pentru securitatea cibernetică**, www.sri.ro, accesat în data de 12.10.2019;
5. **Glosar de termeni pentru domeniul securității cibernetice**, www.sri.ro, accesat în data de 12.10.2019;
6. **Teza de doctorat (rezumat) cercetări privind securitatea sistemelor automate**, autor Ing. Emil Pricop, Ploiești 2017;
7. **Securitatea reţelelor: Metode de atac şi protecţie**, Realizat: Neagaru Daniel, Coteţ Dumitru, Chișinău 2010;
8. https://ro.wikipedia.org/wiki/Securitatea_rețelelor_de_calculatoare, accesat în data de 13.10.2019;
9. http://www.referatele.com/informatica/Amenintari-de-securitate-a-ret419.php, accesat în data de 13.10.2019;
10. https://ramonnastase.ro/blog/exemple-de-atacuri-cibernetice-metode-de-hacking-din-internet, accesat în data de 13.10.2019;
11. http://muhaz.org/proiect-cofinanat-din-fondul-social-european-n-cadrul-pos-dru-v9.html?page=4, accesat în data de 14.10.2019;
12. **Curs. Rețele de calculatoare**, București 2017. Universitatea Politehnică din București http://tet.pub.ro/pages/RC/Retele%20de%20Calculatoare%20-%20Curs.pdf, accesat în data de 16.10.2019;
13. **Teză de doctorat, Contribuţii privind monitorizarea securităţii reţelelor de calculatoare**, Ing. Nicu-Sebastian NICOLĂESCU, Conducător ştiinţific: Prof. Dr. Ing. Victor-Valeriu Patriciu, București 2011. https://docplayer.net/53292411-Teza-de-doctorat-contributii-privind-monitorizarea-securitatii-retelelor-de-calculatoare-romania-academia-tehnica-militara.html), accesat în data de 20.10.2019;
14. https://db-ip.com, accesat în data de 20.10.2019;
15. https://www.nume.ro/cele-mai-bune-instrumente-siem, accesat în data de 20.10.2019;
16. https://softline.ro/solutions/securitate/siem, accesat în data de 20.10.2019;
17. https://ru.wikipedia.org/wiki/SIEM, accesat în data de 20.10.2019;