UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE POLITEHNICA BUCUREȘTI

Şcoala Doctorală de Electronică, Telecomunicații și Tehnologia Informației

Decizie nr. ____ din __-__-____

REZUMAT TEZĂ DE DOCTORAT

Ing. Maria-Mădălina ANDRONACHE

TEHNICI DE ANALIZĂ A TRAFICULUI ÎN REȚELELE DE CALCUL

TRAFFIC ANALYSIS TECHNIQUES IN COMPUTER NETWORKS

COMISIA DE DOCTORAT

Prof. Dr. Ing.	Președinte
Prof. Dr. Ing. Corneliu BURILEANU	Conducător de doctorat
Prof. Dr. Ing.	Referent
Prof. Dr. Ing.	Referent
Dr. Ing.	Referent

BUCUREŞTI 2025

Cuprins

Capitolul 1

Introducere

Informația transportată prin intermediul internetului a devenit unul dintre cele mai importante aspecte ale secolului 21. Practic, prin intermediul acestei unelte, s-a schimbat modul în care persoanele comunică între ele, se distrează, lucrează, fac cumpărături, etc. Astfel, diversele activități ce solicitau un timp suplimentar pentru realizare, au devenit mult mai facile și mai comode.

În contextul de securitate actual, monitorizarea rețelelor a devenit o necesitate. Prin urmare, detectarea incidentelor de securitate sau a anomaliilor dintr-o rețea devin scopul principal deservit de către o monitorizare corespunzătoare.

Având în vedere creșterea gradului de intruziune a atacurilor și a faptului că acestea sunt extrem de dăunătoare, chiar dacă pot părea inofensive, este absolut esențial ca politicile de securitate să fie mai restrictive, iar privilegiile utilizatorilor să nu fie acordate inutil. În această lucrare, se realizează o privire de ansamblu asupra tehnologiilor existente ce pot asigura o monitorizare eficientă a rețelei și se iau în considerare și schimbările provocate de noile tehnologii precum IoT, SDN, etc.

1.1 Prezentarea domeniului tezei de doctorat

Securitatea cibernetică, în era digitală de continuă expansiune, a devenit un aspect critic în protejarea resurselor din zona de tehnologie a informației (date sensibile, confidențialitatea utilizatorilor). Ținând cont și de dependința continuă de tehnologie și de nevoia de digitalizare a tuturor tipurilor de servicii și infrastructuri, amenințările cibernetice au evoluat mult, la nivel volumetric și la nivelul metodelor de sofisticare și mascare a intenției reale.

Aceste tipuri de atacuri nu vizează doar utilizatorii obișnuiți, ci mai ales diverse organizații sau instituții, diverse tipuri de infrastructuri critice și diverse tehnologii ale căror date sunt importante.

Autorii atacurilor sunt, deseori, actori rău intenționați, însă există și situații în care aceștia se grupează sau sunt angajați de către diverse state. Scopul acestora este de a detecta diverse vulnerabilități și de a analiza diverse medii nesecurizate

corespunzător pentru realizarea unor furturi de informații sau a unor daune majore asupra unui/unor sistem/sisteme.

Metodele acestora includ tehnici de phising, atacuri cu fișiere malițioase și chiar și atacuri de tip DoS (Denial-of-Service).

În aceste condiții, analiza traficului de rețea joacă un rol esențial în înțelegerea modului prin care atacurile sau amenințările cibernetice funcționează. Captarea, identificarea și testarea codului malițios permit administratorilor de securitate să determine scopul, metodele de propagare și tehnicile de evitare a detecției utilizate de atacatori.

1.2 Scopul tezei de doctorat

Scopul acestei lucrări este dat de identificarea celor mai bune metode de captare și de analiză a evenimentelor din rețea. Și pentru acest aspect, au fost luate în considerare mai multe metode și tehnici care să conducă la o eficiență sporită atât la nivelul detecției, cât și la nivelul metodelor de prevenție împotriva unor astfel de evenimente.

Prin aceste metode se pot extrage indicatori de compromitere (IoC), se pot construi semnături de detecție și pot elabora strategii de răspuns adaptate fiecărui tip de atac. În plus, informațiile obținute contribuie la îmbunătățirea continuă a sistemelor de detecție automată, la dezvoltarea de politici de securitate mai eficiente și la instruirea echipelor de răspuns la incidente.

Astfel, prin metodele de analiză a traficului se poate construi o componentă strategică a apărării proactive, într-un mediu digital aflat sub presiunea constantă a amenințărilor emergente.

1.3 Conținutul tezei de doctorat

În cadrul acestei lucrări sunt prezentate 8 capitole diferite, ce prezintă diverse abordări ale diverselor metode de analiză a traficului de rețea, atât legitim, cât și malițios.
Structura lucrării cuprinde mai multe capitole, ce vor fi detaliate în cadrul paragrafelor următoare.

În Capitolul 1, au fost prezentate noțiunile introductive ale tezei și domeniul de securitate cibernetică.

În cadrul Capitolului 2, au fost prezentate informațiile asupra mediului actual de securitate cibernetică, precizându-se domeniile conexe precum cel de învățare automată, de analiză statică și dinamică, dar și de sisteme de Management al Evenimentelor și al Informațiilor de Securitate.

În Capitolul 3 au fost identificate soluțiile software actuale și au fost analizate beneficiile și limitările fiecăreia dintre acestea, pe baza informațiilor din literatură.

Capitolul 4 a cuprins primul set de analize efective a domeniului de malware, utilizându-se tehnici de învățare automată și baze de date publice preetichetate, în scopul identificării celor mai buni algoritmi de detecție a intruziunilor.

În Capitolul 5 analiza efectivă a continuat prin intermediul unor fișiere malițioase efective, din zona de resurse publice, ce au fost analizate prin intermediul unor tehnici hibride (de tip static și dinamic).

În Capitolul 6, analiza a continuat cu experimente specifice analizei de evenimente a traficului de rețea, utilizându-se diverse tehnici bazate pe sisteme de tip SIEM.

Capitolul 7 a cuprins integrarea metodelor menționate anterior la nivelul unei infrastructuri de rețea în mediul simulat eve-ng. Prin intermediul acestuia, au fost generate diverse scenarii de atac și diverse metode de identificare a acestora sau de protejare împotriva lor.

În Capitolul 8 au fost introduse principalele concluzii, contribuțiile lucrării și perspectivele de dezvoltare ulterioară, alături de lista de lucrări publicate pe parcursul programului doctoral.

Capitolul 2

Securitatea rețelelor de calculatoare

Securitatea rețelelor este un ansamblul de politici, tehnologii și practici implementate pentru a proteja integritatea, confidențialitatea și disponibilitatea datelor și a serviciilor într-o infrastructură de comunicații. În esență, securitatea rețelelor are rolul de a preveni accesul neautorizat sau modificarea și distrugerea informațiilor transmise printr-o rețea. Amenințările cibernetice sunt constante și complexe și, astfel, pot conduce la intruziuni și furturi de informații cheie. Prin urmare, securitatea rețelelor implică un set diversificat de mecanisme, inclusiv firewall-uri, sisteme de detecție și prevenție a intruziunilor (IDS/IPS), segmentarea traficului și monitorizare continuă, prin intermediul soluțiilor de tip SIEM. Mai mult, în cazul în care este identificat un atac, acesta trebuie analizat pentru a înțelege vulnerabilitățile rețelei ce au condus la permiterea acestuia în rețea. Astfel, securitatea rețelelor este un proces dinamic, care trebuie să fie capabil să răspundă în timp real la atacuri complexe.

2.1 Securitatea cibernetică

Securitatea cibernetică vizează protejarea sistemelor informatice, a rețelelor, a dispozitivelor și a datelor împotriva atacurilor digitale, accesului neautorizat, furtului sau deteriorării.

Într-un mediu digital în continuă expansiune, în care aproape toate activitățile sociale, economice și guvernamentale depind de tehnologie, securitatea cibernetică devine o componentă esențială a funcționării sigure și stabile a societății. Scopul principal al acestui concept este de a asigura confidențialitatea, integritatea și disponibilitatea informației, indiferent de forma în care aceasta circulă sau este stocată.

Într-un peisaj marcat de atacuri tot mai sofisticate, securitatea cibernetică nu mai este o opțiune, ci o necesitate strategică pentru protejarea identității și a infrastructurilor.

2.2 Învățarea automată

Tehnicile de învățare automată reprezintă un set de metode prin care sistemele informatice pot învăța automat anumite caracteristici ale unor date și pot lua decizii, pe baza conceptelor învățate, fără a fi explicit programate pentru fiecare situație.

Printre cele mai utilizate tehnici de învățare automată se numără algoritmii de clasificare (Support Vector Machines, k-Nearest Neighbors sau Naive Bayes), care sunt folosiți pentru a eticheta datele în funcție de trăsături observabile.

În contextul securității cibernetice în cadrul rețelelor de comunicații, aceste tehnici sunt adaptate pentru detectarea anomaliilor, identificarea de comportamente malițioase și automatizarea procesului de analiză, oferind o capacitate superioară de reacție la amenințări emergente.

Însă, performanța modelelor învățare automată depinde de calitatea și volumul datelor folosite pentru antrenare, precum și de selecția adecvată a trăsăturilor relevante.

2.3 Analiza statică și analiza dinamică

Analiza statică a malware-ului se referă la examinarea codului sau a fișierului malițios fără a-l executa, având scopul de a înțelege structura și intențiile acestuia, într-un mod controlat și sigur. Această tehnică utilizează instrumente precum decompilatoare, analizatoare de șiruri de date sau de funcții, pentru a identifica semnături cunoscute, secvențe de cod suspecte sau tehnici de ascundere a caracterului real, malițios.

Analiza dinamică presupune rularea software-ului rău intenționat într-un mediu izolat, precum un sandbox, pentru a observa comportamentele acestuia: modificări în regiștri de sistem, conexiuni de rețea sau acțiuni asupra fișierelor. Această tehnică oferă o imagine detaliată asupra efectelor pe care un malware le poate produce într-un sistem real.

Îmbinate, cele două metode permit o înțelegere mai profundă și mai precisă a amenințărilor informatice: analiza statică oferă rapiditate și eficiență inițială, în timp ce analiza dinamică dezvăluie comportamente ascunse.

2.4 Sisteme de tip IDS/IPS

Tehnicile implementate în sistemele IDS (Intrusion Detection System) și IPS (Intrusion Prevention System) sunt concepute pentru a detecta și, respectiv, a preveni activitățile suspecte sau neautorizate, într-o rețea sau într-un sistem informatic.

IDS-urile monitorizează traficul și evenimentele din sistem, semnalând posibile intruziuni, fără a interveni direct.

IPS-urile blochează automat traficul malițios identificat.

Aceste sisteme folosesc două metode principale de detecție: detecția bazată pe semnături, care compară activitatea observată cu o bază de date de atacuri cunoscute, și detecția bazată pe anomalii, care semnalează deviații de la comportamentul normal al sistemului.

2.5 Sisteme de tip SIEM

Sistemele SIEM (Security Information and Event Management) reprezintă soluții centralizate de monitorizare și analiză a evenimentelor de securitate, concepute pentru a oferi vizibilitate în timp real asupra infrastructurii IT.

Aceste sisteme colectează, corelează și analizează date din surse multiple, transformând volume mari de evenimente de rețea în informații utile pentru detectarea amenințărilor și răspunsul la incidente.

Un SIEM eficient folosește reguli de corelare, alerte automate și analize comportamentale pentru a identifica activități suspecte.

Într-un peisaj cibernetic tot mai complex, SIEM devine o componentă esențială pentru operațiunile de securitate, permițând o reacție mai rapidă în fața atacurilor informatice.

2.6 Concluzii

În cadrul acestui capitol, au fost identificate aspectele esențiale ale domeniului de securitate cibernetică și domenii conexe acestuia. Acestea au fost prezentate, prin intermediul mai multor secțiuni, pentru o documentare mai ușoară asupra ideilor cheie necesare pentru înțelegerea experimentelor realizate în cadrul lucrării.

Capitolul 3

Metode de analiză a intruziunilor

Detectarea software-urilor malițioase sau a intruziunilor de rețea presupune identificarea prezenței sau activității codului malițios într-un sistem informatic.

Sistemele de analiză a traficului de rețea includ mai multe etape precum: monitorizare, detecție, analiză și răspuns.

Metodele clasice includ detecția bazată pe semnături, unde fișierele suspecte sunt comparate cu o bază de date de coduri cunoscute, și cea care analizează structura și comportamentul fișierelor, pentru a identifica caracteristici suspecte.

În paralel, detecția bazată pe anomalii monitorizează comportamentul normal al sistemului și semnalează deviații ce pot indica activități malițioase.

Aceste metode clasice sunt îmbunătățite constant cu algoritmi de învățare automată, capabili să recunoască intruziunile, într-un mod mult mai facil.

Detectarea eficientă implică adesea o combinație între analiza statică, analiza dinamică și contextualizarea comportamentului, într-un cadru mai larg de securitate.

3.1 Soluții de analiză generală a traficului de rețea

Metodele de analiză a traficului de rețea includ jurnalizări ale evenimentelor, ce trebuie analizate.

Totuși, pentru identificarea vulnerabilităților dintr-o rețea, este nevoie de analiza acestora prin intermediul a mai multe instrumente. O parte dintre acestea sunt:

1. Nmap și Nessus – care oferă informații despre vulnerabilități, porturi și servicii deschise.

2. Wireshark și tcpdump – ce pot analiza de pachete de rețea pentru capturarea și inspectarea traficului de rețea.

3. NetFlow Analyzer – ce permite o analiză a fluxurilor de rețea, pentru monitorizarea performanței și identificarea anomaliilor.

4. Suricata – care este un sistem de detecție și prevenire a intruziunilor (IDS/IPS) ce analizează traficul de rețea în timp real.

5. Snort – care este un sistem IDS/IPS open-source pentru detectarea și prevenirea atacurilor în rețea.

3.2 Soluții bazate pe Învățarea automată

În timp ce tehnologiile de învățare automată pot aduce un avantaj semnificativ în detecția rapidă a atacurilor, aplicarea acestora în securitatea cibernetică presupune, totodată, provocări semnificative

Instrumente și soluții pentru Învățarea automată sunt:

1. WEKA – platformă de învățare automată care include algoritmi pentru clasificare sau regresie.

2. Scikit-learn – bibliotecă de învățare automată pentru Python, cu algoritmi pentru clasificare sau regresie.

3.3 Soluții bazate pe analiza statică și dinamică

Analiza statică cuprinde mai multe concepte cheie precum inspecția de semnături, analiza metadatelor sau verificarea structurii unor fișiere.

Soluții utilizate in cadrul acestui capitol sunt:

1. PEStudio – detectează informații despre structura fișierelor si importurile malițioase folosite de către fișiere executabile.

2. IDA Pro / Ghidra – soluții de tip decompilator pentru analiza fișierelor la nivel de cod de asamblare.

3. Strings – soluție ce extrage șiruri din cadrul fișierelor binare, utile pentru identificarea de indicatori de compromitere.

4. YARA – metodă ce permite definirea de reguli pentru identificarea fișierelor cu caracteristici similare unui fișier malițios deja cunoscut.

5. VirusTotal – bază de date ce agregă rezultate de la zeci de motoare antivirus și permite analiza comportamentală.

Analiza dinamică presupune rularea efectivă a fișierului malițios, într-un mediu izolat, pentru identificarea caracteristicilor sale comportamentale.

Soluții utilizate in cadrul acestei analize sunt:

1. Procmon – monitorizează procese și activități ale sistemului în timp real.
2. Wireshark – analizează traficul de rețea generat de malware pentru a detecta exfiltrarea datelor sau conexiuni la servere de comandă și control (C2).
3. Antivirusuri – soluții cu detecții automate ce capabilități avansate de identificare comportamentală intruzivă.
4. Strace – este un tool de sistem Linux ce poate monitoriza interacțiunile unui fișier cu sistemul de operare

3.4 Soluții bazate pe SIEM

Sistemele de management al evenimentelor și informațiilor de securitate (SIEM) pot colecta date din diverse surse, cu scopul îmbunătățirii detectării activității suspecte în rețea.

Soluții de tip SIEM considerate în această lucrare sunt:

1. OSSEC – sistem de detecție a intruziunilor open-source cu funcționalități de analiză a logurilor.
2. OSSIM – platformă open-source care integrează multiple instrumente pentru colectarea, corelarea și analiza datelor de securitate din rețea.
3. Wazuh – soluție open-source de monitorizare a securității care extinde capabilitățile OSSEC, adăugând funcționalități avansate de analiză, detecție a intruziunilor și gestionare a incidentelor într-un mediu distribuit.

3.5 Concluzii

În cadrul acestui capitol au fost analizate principalele soluții existente pentru analiza intruziunilor. Astfel, acestea au fost analizate comparativ, identificându-se, prin intermediul literaturii, avantajele și dezavantajele fiecărei soluții, în parte.

Capitolul 4

Detecția anomaliilor din cadrul unei rețele, prin intermediul tehnicilor de învățare automată

În securitatea cibernetică, învățarea automată joacă un rol esențial datorită capacității sale de a identifica modele complexe și de a detecta și răspunde amenințărilor într-un mod mai rapid decât metodele tradiționale. Acesta permite soluțiilor de securitate să se adapteze continuu la noi tipuri de amenințări, îmbunătățind astfel prevenirea și răspunsul la incidentele cibernetice.

4.1 Modul de utilizare a tehnicilor de învățare automată pentru detecția anomaliilor

Utilizarea învățării automate în detectarea malware-ului presupune antrenarea unor modele care pot învăța să distingă între fișiere sau comportamente malițioase și cele legitime, pe baza unor caracteristici extrase din datele de intrare.

Procesul începe cu colectarea unui set mare de date etichetate, care include fișiere malware și non-malware, și extragerea unor trăsături relevante.

Modelele de învățare automată sunt antrenate pe aceste trăsături, pentru a învăța tiparele asociate fiecărui tip de fișier.

După antrenament, modelul poate clasifica noi fișiere sau poate fi evaluat prin intermediul unor indici de performanță prestabiliți.

4.2 Identificarea anomaliilor de trafic prin intermediul WEKA

WEKA este o platformă utilizată pe scară largă pentru aplicații ce includ învățarea automată, având implementați o gamă largă de algoritmi de clasificare diferiți.

În cadrul acestui capitol este utilizată o bază de date publică, ce este testată prin intermediul mai multor algoritmi diferiți, așa cum reiese și din Figura 4.1.

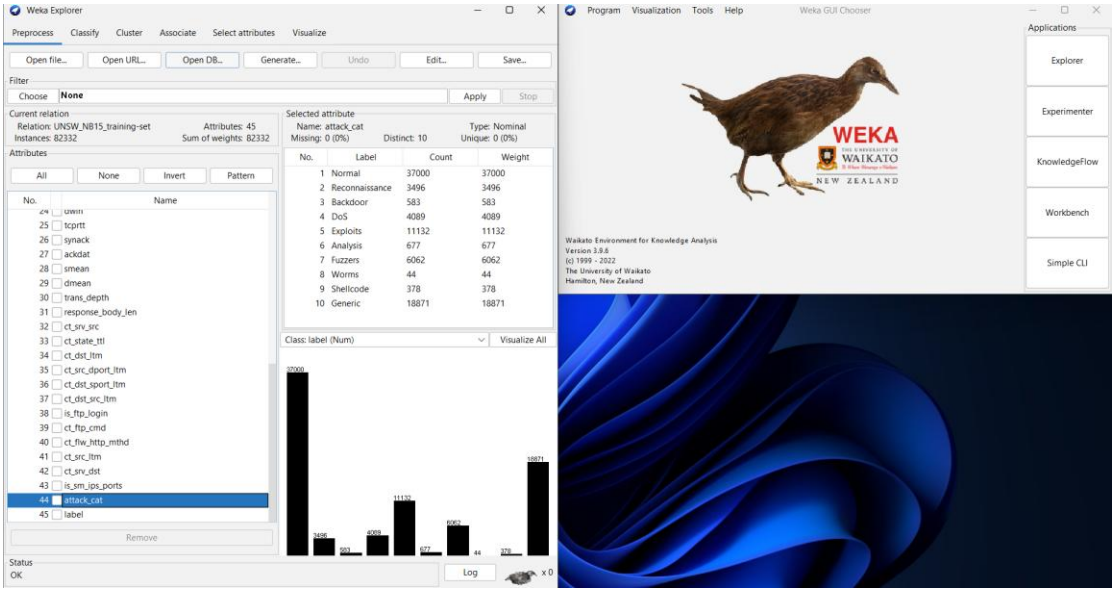


Figura 4. 1: *Încărcarea bazei de date în cadrul soluției WEKA*

4.3 Identificarea anomaliilor de trafic prin intermediul Scikit-learn

Scikit-Learn este o soluție software ce include o colecție de biblioteci care pot implementa algoritmi de învățare automată.

În cadrul acestui capitol este utilizată aceeași bază de date, ca în cazul anterior, ce este testată prin intermediul unui program în Python, ce include și biblioteci Scikit-learn. Modul prin care sunt realizate funcțiile, în cadrul acestui capitol, este redat în Figura 4.4.

```
from sklearn.neural_network import MLPClassifier
classifier = MLPClassifier(
    hidden_layer_sizes=(100,)
    learning_rate_init=0.3,
    momentum=0.2,
    max_iter=500,
    verbose=False,
    random_state=0,
    early_stopping=True,
    n_iter_no_change=20
)
classifier.fit(X_train, y_train)
```

Figura 4. 2*: Metoda de test utilizată în Python cu Scikit Learn*

4.4 Analiză comparativă asupra rezultatelor obținute prin intermediul celor două soluții

Analiza comparativă, realizată în cadrul acestui capitol include o multitudine de parametri de performanță, de metode de împărțire a datelor și de algoritmi de învățare automată, similar cu reprezentarea din Figura 4.9.

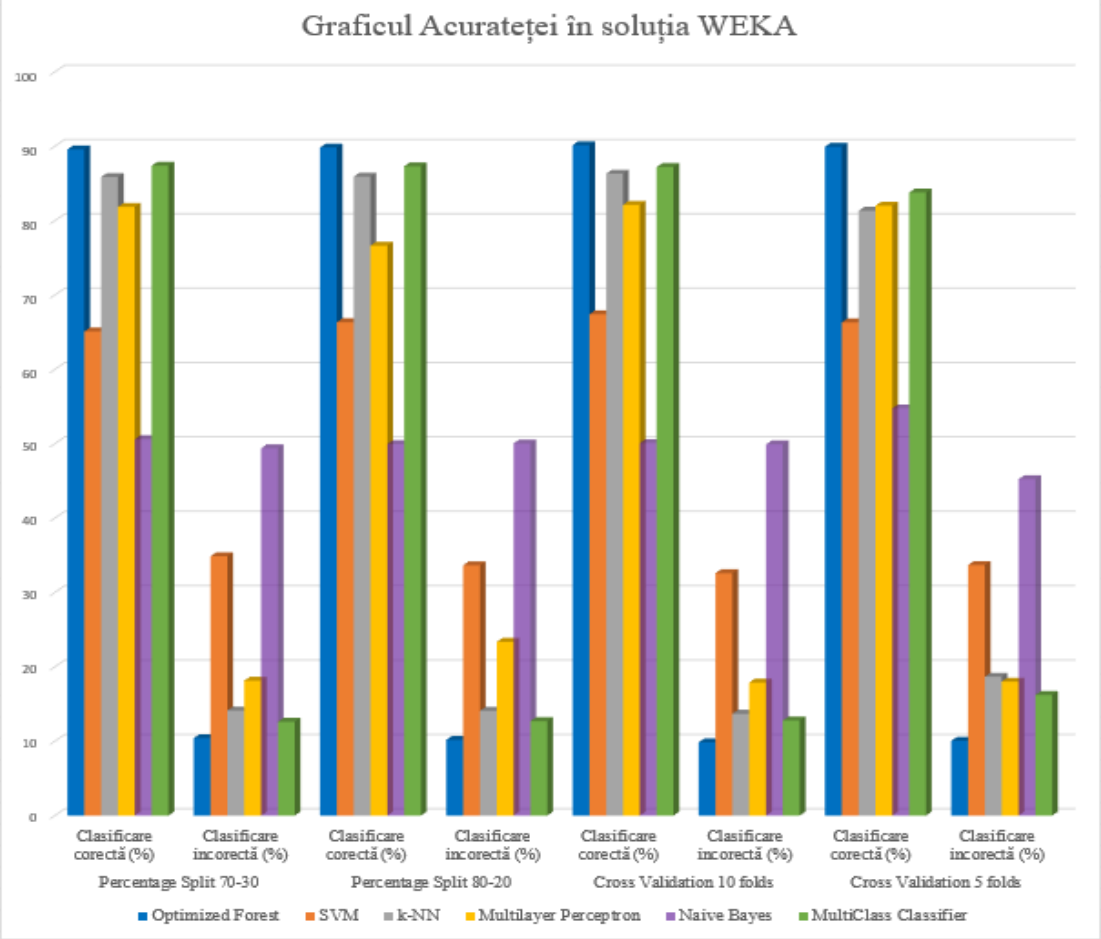


***Figura 4. 3**: Graficul parametrului de acurateţe în cadrul soluției WEKA*

4.5 Concluzii și contribuții originale

În cadrul acestui capitol, au fost analizate comparativ cele două soluții, ce implementează concepte de învățare automată.

Contribuția originală esențială a fost că, pe parcursul capitolului, au fost identificați cei mai mulți algoritmi de clasificare a informațiilor pentru setul de date utilizat și a fost realizată o analiză comparativă a acestora, luând în considerare mai mulți indici de performanță.

Capitolul 5

Detecția caracteristicilor unui fișier malițios din cadrul unei rețele, prin intermediul metodelor de analiză statică și dinamică

Analiza hibridă în securitatea cibernetică combină abordările bazate pe analiza statică și analiza dinamică. Prin integrarea acestor soluții, se pot obține rezultate mai precise și o mai bună gestionare a incidentelor, oferindu-se date ce pot conduce la o protecție completă și un răspuns mai rapid la atacuri.

5.1 Fișierele malițioase utilizate în analiza statică și dinamică

Fișierele malițioase din cadrul acestui capitol sunt caracteristice zonei de resurse de internet și cuprind eșantioane precum cele din Tabelul 5.1.

Adware	**A1**	04789bb1e63b81997e53786d1f19a6dde477b29b54ad5bcb12aeb9bce3d0f72b [1]
Malware	**M1**	ef93353c2ecc677d4db0854d9eac80717a496af273ee0f2f5a21fda5682e248e [2]

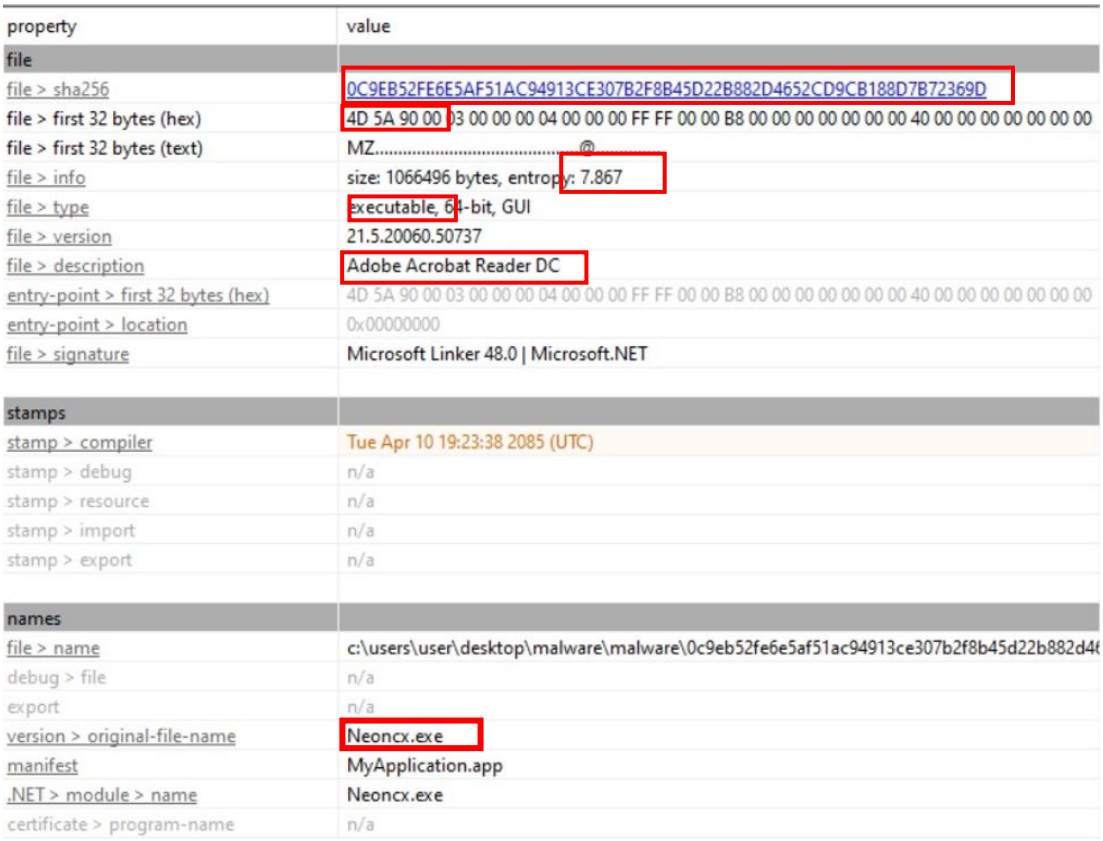
Tabelul 5. 1: *Fișierele malițioase analizate*

5.2 Utilizarea analizei statice pentru detecția anomaliilor

Examinarea fișierelor prin intermediul acestei analize cuprinde mai multe etape precum: colectarea informațiilor, identificarea conceptelor cheie și descompunerea codului. Toate aceste etape sunt analizate și detaliate în cadrul acestui capitol, cu scopul identificării unui mod de lucru coerent pentru realizarea experimentelor.

5.3 Identificarea caracteristicilor malițioase ale unui fișier, prin intermediul analizei statice

În cadrul datelor experimentale, fișierele sunt analizate utilizând mai multe tool-uri, ce identifică diverse tipuri de caracteristici precum cele din Figura 5.3.



property	value
file	
file > sha256	0C9EB52FE6E5AF51AC94913CE307B2F8B45D22B882D4652CD9CB188D7B72369D
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file > first 32 bytes (text)	MZ.....@.....
file > info	size: 1066496 bytes, entropy: 7.867
file > type	executable, 64-bit, GUI
file > version	21.5.20060.50737
file > description	Adobe Acrobat Reader DC
entry-point > first 32 bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
entry-point > location	0x00000000
file > signature	Microsoft Linker 48.0 | Microsoft.NET
stamps	
stamp > compiler	Tue Apr 10 19:23:38 2085 (UTC)
stamp > debug	n/a
stamp > resource	n/a
stamp > import	n/a
stamp > export	n/a
names	
file > name	c:\users\user\desktop\malware\malware\0c9eb52fe6e5af51ac94913ce307b2f8b45d22b882d4(
debug > file	n/a
export	n/a
version > original-file-name	Neoncx.exe
manifest	MyApplication.app
.NET > module > name	Neoncx.exe
certificate > program-name	n/a

***Figura 5. 1**: Modul prin care fișierul malware S1 este analizat prin intermediul soluției PEStudio*

5.4 Utilizarea analizei dinamice pentru detecția anomaliilor

Analiza dinamică cuprinde, din punct de vedere experimental, efectuarea unor pași precum: configurarea mediului de test, analiza interacțiunii fișierului malițios cu diverse aspecte de sistem și identificarea caracteristicilor de comportament asociate acestor interacțiuni.

Toate aceste etape sunt analizate și detaliate în cadrul acestui capitol, cu scopul identificării unui mod de lucru coerent pentru realizarea experimentelor.

5.5 Identificarea caracteristicilor malițioase ale unui fișier, prin intermediul analizei dinamice

În cadrul datelor experimentale, fișierele sunt analizate utilizând mai multe tool-uri, ce identifică diverse tipuri de caracteristici precum cele din Figura 5.11.

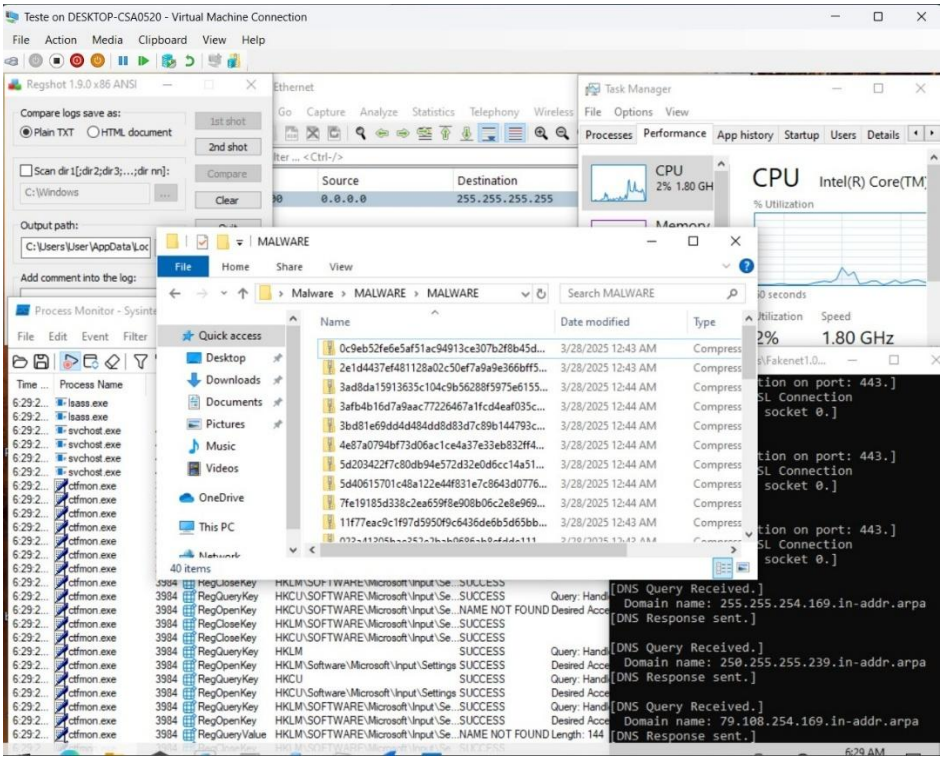


Figura 5. 11: *Modul de efectuare a analizei dinamice, alături de instrumentele și eșantioanele utilizate*

5.6 Concluzii și contribuții originale

Prin intermediul acestui capitol, au fost analizate mai multe tipuri de fișiere malițioase. Funcționalitatea acestora a fost testată atât prin intermediul analizei statice, fără execuția fișierului, cât și prin intermediul analizei dinamice, cu rularea acestuia într-un mediu controlat.

Contribuția originală cheie a fost dată de identificarea caracteristicilor malițioase pe baza mai multor soluții complementare și analiza acestora, din punct de vedere comparativ, cu scopul efectuării unei caracterizări cât mai complete a unui anumit tip sau a unei familii de malware.

Capitolul 6

Detecția unui trafic sau program malițios din cadrul unei rețele, prin intermediul sistemelor de tip SIEM

Sistemele SIEM (Security Information and Event Management) sunt utilizate în detectarea malware-ului prin centralizarea, corelarea și analiza în timp real a datelor generate de diferite componente ale infrastructurii IT. Acesta colectează jurnale și alerte de securitate, le corelează și le analizează pentru a identifica activități suspecte asociate cu prezența malware-ului. Prin aceste metode, un SIEM permite echipelor de securitate să detecteze rapid atacurile malware, să investigheze contextul acestora și să răspundă eficient pentru a limita impactul asupra organizației.

6.1 Utilizarea soluției SIEM OSSEC

Sistemul OSSEC este o soluție de tip SIEM care funcționează pe principiul Agent-Manager, colectând logurile din mai multe surse și integrându-le, în mod centralizat, pentru analiză ulterioară.

Avantajele date de OSSEC sunt faptul că este un sistem open-source și faptul că poate fi considerat un mediu tehnologic propice învățării.

Dezavantajele date de această soluție includ instabilitatea platformei, deconectări frecvente ale agenților și o interfață grafică ce se întrerupe frecvent.

Pe parcursul capitolului, au fost analizate și alte avantaje și limitări ale soluției.

6.2 Utilizarea soluției SIEM OSSIM

OSSIM, dezvoltat și susținut de AlienVault, reprezintă una dintre cele mai mature soluții open-source în domeniul securității cibernetice, oferind un cadru integrat pentru colectarea, corelarea și analiza evenimentelor.

Un alt avantaj major al soluției este constituit de interfața grafică deoarece aceasta permite mai multe modului de vizualizare al alertelor și chiar grafice dinamice.

Unul dintre principalele dezavantaje concluzionate prin intermediul experimentelor au fost date de complexitatea destul de mare a sistemului OSSIM în zona de instalare.

Pe parcursul capitolului, au fost analizate și alte avantaje și limitări ale soluției.

6.3 Utilizarea soluției SIEM WAZUH

Wazuh este o soluție de tip SIEM derivată din OSSEC, dar semnificativ îmbunătățită în ceea ce privește funcționalitățile.

Un avantaj al acestei soluții provine din faptul că este foarte versatilă în ceea ce ține de înregistrarea logurilor din diverse echipamente de rețea sau chiar diverse tipuri de aplicații.

Un adezavantaj este dat de consumul ridicat de resurse necesare pentru instalare și configurarea inițială.

Pe parcursul capitolului, au fost analizate și alte avantaje și limitări ale soluției.

6.4 Analiza comparativă a performanțelor sistemelor de tip SIEM analizate

În urma analizei comparative asupra metodelor de tip SIEM utilizate, s-au identificat avantajele și dezavantajele vizualizate experimental.

Conform acestui fapt, a fost realizată și o ierarhie a performanțelor fiecărui sistem.

6.5 Concluzii și contribuții originale

Concluziile acestui capitol au constat în identificarea celui mai potrivit sistem SIEM pentru monitorizarea și caracterizarea evenimentelor din cadrul unei rețele.

Contribuția originală principală a fost dată de testarea comparativă a acestor soluții și de identificare a limitărilor și avantajelor fiecărei soluții, în parte.

Capitolul 7

Detecția anomaliilor sau a fișierelor malițioase în cadrul traficului de rețea uzual

Monitorizarea constantă a evenimentelor din rețea conduce, implicit, și la o detecție eficientă a anomaliilor înregistrate la nivelul acesteia.

Procesul de detecție a acestora cuprinde anumite etape care se bazează pe tehnici avansate de analiză a datelor sau de învățare automată precum:

1. Colectarea datelor din rețea
2. Crearea modelelor de trafic normal
3. Detectarea anomaliilor

7.1 Arhitectura rețelei

Pentru realizarea unor scenarii de test eficiente, a fost realizată p arhitectură de rețea complexă, ce poate fi regăsită prin intermediul Figurii 7.1.

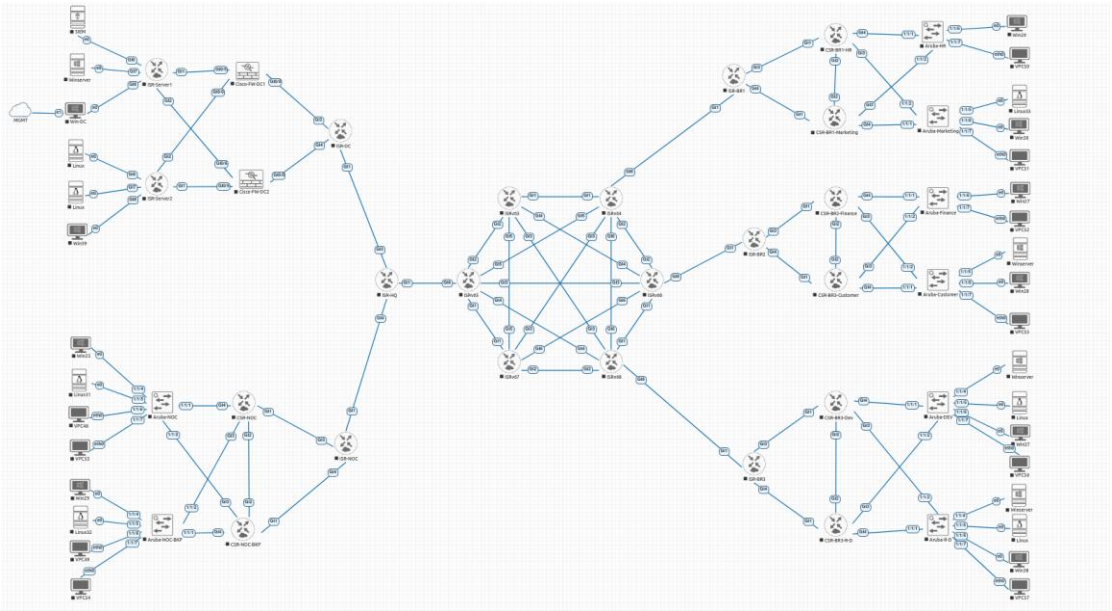


***Figura 7. 1**: Arhitectura generală a rețelei analizate*

7.2 Simularea atacurilor cibernetice la nivel de rețea

Atacurile cele mai probabile de la nivelul unei rețele sunt: scanări ale rețelei, identificări de atacuri de tip inundare a acesteia sau de atacuri de tip Denial of Service (DoS).

Toate acestea sunt reprezentate experimental prin intermediul acestui capitol.

7.3 Simularea atacurilor cibernetice prin intermediul fișierelor malițioase

În cadrul acestui capitol, tot prin intermediul mediului virtualizat eve-ng, a fost creat un scenariu realist în care au fost simulate infectări cu fișiere malițioase, care sunt mascate în fișiere legitime și care sunt executate în rețea.

Simulările au inclus execuția mai multor tipuri de fișiere malițioase precum ransomware, spyware, malware, etc.

7.4 Analiza statică a fișierelor malițioase utilizate

În cadrul acestui capitol, au fost analizate toate tipurile de fișiere executate anterior, atât pentru zona de sistem de operare Ubuntu, cât și pentru zona sistemului de operare Linux.

În acest mod, au fost extrase caracteristicile principale ale fiecărui tip de fișier, în parte.

7.5 Analiza fișierelor malițioase utilizate utilizând tehnici de Machine-Learning

În contextul arhitecturii de rețea utilizată, soluțiile de tip WEKA sau integrarea proceselor cu biblioteci din Scikit-learn se face pentru a corela diverse evenimente și pentru a învăța diverse modele de comportament normal. Acest mod de lucru presupune exportul unor fișiere de trafic din cadrul sistemului de tip SIEM, curățarea acestora și introducerea lor în cadrul soluțiilor de învățare automată, pentru analiză.

7.6 Modul de analiză al traficului de rețea

Pe parcursul acestui capitol, dar și pe parcursul acestei lucrări, au fost prezentate mai multe moduri de analiză a traficului de rețea, cu scopul detecției diverselor intruziuni și a găsirii celor mai potrivite soluții de securitate, pentru un mediu de rețea real.

7.7 Concluzii și contribuții originale

În cadrul acestui capitol, a fost realizată o infrastructură de rețea proprie, ce a inclus și diverse metode de analiză a traficului. Tot prin arhitectura de rețea propusă, au fost simulate și diverse atacuri sau execuții ale fișierelor malițioase, al căror caracteristici și comportament a fost analizat, prin intermediul tuturor tehnicilor menționate în capitolele anterioare.

Contribuția majoră constă în crearea mediului de test și analiza comparativă a intruziunilor.

Concluzii

Lucrarea prezentă a utilizat mai multe tehnici de analiză a traficului de rețea și poate fi constituită o bază solidă în realizarea unei analize concrete și corecte de cercetare a domeniului de securitate, pe niveluri diferite de intruziune.

8.1 Rezultate obținute

Rezultatele obținute sunt prezentate schematic astfel:

1. În Primul Capitol, s-au conștientizat aspectele cheie ale lucrării.
2. În Capitolul 2, s-au prezentat aspectele teoretice și noțiunile esențiale ale acestora.
3. Din Capitolul 3 a rezultat înțelegerea modului de funcționare al tehnologiilor utilizate în domeniul securității cibernetice.
4. În Capitol 4, rezultatul a constat în identificarea unor algoritmi de învățare automată ideali pentru detecția intruziunilor.
5. Din Capitolul 5 a rezultat înțelegerea caracteristicilor cheie în funcționarea unui fișier malițios.
6. La nivelul Capitolului 6 s-a identificat modul de funcționare al intruziunilor de rețea, captate prin intermediul unui sistem SIEM.
7. În Capitolul 7 au fost introduse toate metodele de analiză anterioare pentru detecția unor intruziuni în cadrul unei arhitecturi de rețea proprii.

8.2 Contribuții originale

Contribuțiile originale ale acestei lucrări au fost obținute atât prin zona de documentare asupra contextului actual de securitate cibernetică, cât și prin intermediul implementării în medii reale sau simulate a diverselor scenarii de test, pentru obținerea de rezultate experimentale. Toate acestea pot fi divizate astfel:

1. Analiza comparativă a soluțiilor de tip open-source și identificarea celor care să fie testate și la nivel experimental.

2. Efectuarea experimentelor bazate pe soluții de tip Machine-Learning, utilizându-se WEKA și limbajul de programare Python, prin intermediul cărora au fost implementate diverse funcții și biblioteci din zona Scikit-learn. Aceste experimente au fost multiple, utilizându-se diverse metode de testare și

diverși parametri de analiză și indici de performanță, cu scopul definirii unei ierarhii a celor mai buni algoritmi de clasificare a unor seturi de date ce conțineau și intruziuni.

Articole: 1. ***Performance Comparison of Malware Classification Algorithms using WEKA Tool***

1. ***Performance Comparison of Malware Classification Algorithms using WEKA Tool***
2. ***Intrusive application detection using WEKA classifiers***

3. Implementarea unei arhitecturi bazate pe mediu virtual, care să poată cuprinde analiza soluțiilor de tip open-source și includerea unui IDE (Integrated development environment), prin intermediul cărora să poată fi realizate experimentele ce includ Machine-Learning, în limbajul de programare Python.

4. Efectuarea unei analize hibride, statică și dinamică, asupra mai multor tipuri de fișiere malițioase diferite, reliefându-se aspectele cheie de impact al acestora, în sisteme de operare Linux și Windows. De asemenea, au fost extrase și analizate comparativ aspectele definitorii ale acestora, atât din punct de vedere structural, cât și din punct de vedere experimental, pentru a putea face o caracterizare completă a modului prin care acestea pot infecta o rețea de calculatoare.

Articole: 1. ***A Malware Study using Static and Dynamic Analysis***

2. ***The Impact of Malware Attacks on the Performance of Various Operating Systems***

5. Testarea diverselor soluții de analiză statică și dinamică, atât din punct de vedere comparativ, cât și din punct de vedere al identificării a cât mai multor informații cheie, ce pot defini anumite fișiere malițioase.

6. Implementarea unei arhitecturi bazate pe mediu virtual, care să cuprindă analiza soluțiilor de tip analiză statică și dinamică. Prin urmare, au fost create medii izolate, care să influențeze cât mai puțin mediul de producție, dar care să poată simula un mediu real.

7. Implementarea unei arhitecturi de rețea, ce a inclus mai multe mașini virtuale a căror loguri de rețea erau monitorizate prin intermediul unei soluții de tip SIEM de tip agent-manager. Prin intermediul acestei arhitecturi au fost testate diverse tipuri de atacuri, ce erau monitorizate și afișate prin intermediul unei interfețe grafice. Toate acestea au inclus atât sistemul de operare Windows, cât și sistemul de operare Linux.

Articole: 1. ***A comparative study of intrusion events in different SIEM systems***

2. ***Analyzing Network Anomalies Using Wazuh SIEM***

8. Testarea diverselor soluții de tip SIEM din punct de vedere comparativ, pentru a identifica cel mai bun mod de monitorizare a evenimentelor din rețea și pentru a identifica diverse avantaje și dezavantaje ale acestora.

9. Implementarea unei arhitecturi de rețea proprii, ce a inclus atât elemente de configurare echipamente de rețea, cât și moduri diferite de comunicare a resurselor. Acestea au fost incluse într-un mediu de tip eve-ng, respectându-se principii de segmentare și de acces diferențiat la diverse tipuri de resurse.

10. Pe baza arhitecturii de rețea realizată anterior, au fost incluse soluții de tip Management a Evenimentelor și Informațiilor de Securitate, au fost realizate diverse scenarii de atac, utilizând atacuri de rețea obișnuite și atacuri de rețea bazate pe diverse tipuri de fișiere malițioase. Toate aceste intruziuni au fost, ulterior, analizate în cadrul aceleiași rețele, pentru a fi definite caracteristicile definitorii ale acestora.

Articole: ***Strategic Management and Oversight of Security Events in a Business Organization***

11. Prin intermediul arhitecturii de rețea au fost analizate diverse fișiere malițioase, din punct de vedere static și dinamic și au fost identificate și moduri de implementare a soluțiilor de învățare automată, care să poată fi incluse în mediul de test.

12. Pe tot parcursul lucrării, au fost definite și implementate diverse măsuri de protecție la intruziuni, ce rezultau în urma experimentelor realizate.

Aceste contribuții pot influența conștientizarea complexității mediului de securitate cibernetică și pot conduce la optimizarea anumitor procese și metode direct implicate în acesta.

8.3 Lista lucrărilor originale

Pe parcursul activității de cercetare din cadrul stagiului doctoral, autorul a publicat un număr de 7 lucrări științifice legate de domeniul tezei de doctorat, din care 7 ca prim autor și 4 indexate în IEEEXplore:

L.1. **"*Strategic Management and Oversight of Security Events in a Business Organization*"**

Autori: **Maria-Mădălina Andronache**, Alexandru Vulpe, Corneliu Burileanu

Anul publicării: 2025

Revistă: *UPB Scientific Bulletin, Series C: Electrical Engineering and Computer Science*

Stadiu: acceptat, în curs de publicare

L.2. ***" A Comparative Study of Intrusion Events in Different SIEM Systems"***

Autori: **Maria-Mădălina Andronache**, Alexandru Vulpe, Corneliu Burileanu

Anul publicării: 2025

Conferință: *IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Stará Lesná, Slovakia, 2025, (**IEEEXplore**);

Stadiu: publicat, pp. 000065-000070, doi: 10.1109/SAMI63904.2025.10883178.

L.3. ***"The Impact of Malware Attacks on the Performance of Various Operating Systems"***

Autori: **Maria-Mădălina Andronache**, Alexandru Vulpe, Corneliu Burileanu

Anul publicării: 2024

Revistă: **International Journal of Advanced Computer Science and Applications (IJACSA)**, Vol. 15, No. 12, 2024 (**Q3**), **WOSUID**: **WOS:001394195600001**;

Stadiu: publicat, doi: 10.14569/IJACSA.2024.0151257

L.4. ***"Analyzing Network Anomalies Using Wazuh SIEM"***

Autori: **Maria-Mădălina Andronache**, Alexandru Vulpe, Corneliu Burileanu

Anul publicării: 2024

Conferință: WWW/Internet 2024 Conference, Zagreb, Croatia,

Stadiu: publicat, Proceedings of the International Conferences on Applied Computing 2024 and WWW/Internet 2024, 2024, pp 381-385, ISBN (Book): 978-989-8704-62-7

L.5. ***"A Malware Study using Static and Dynamic Analysis"***

Autori: **Maria-Mădălina Andronache**, Alexandru Vulpe, Corneliu Burileanu

Anul publicării: 2024

Conferință: International Conference on Communications (COMM) 2024, Bucharest, Romania, **IEEEXplore**;

Stadiu: publicat, pp. 1-6, doi: 10.1109/COMM62355.2024.10741424.

L.6. ***"Performance Comparison of Malware Classification Algorithms using WEKA Tool"***

Autori: **Maria-Mădălina Andronache**, Alexandru Vulpe, Corneliu Burileanu

Anul publicării: 2024

Conferință: International Conference on Electronics, Computers and Artificial Intelligence (ECAI) 2024, Iași, Romania, **IEEEXplore;**

Stadiu: publicat, pp. 1-6, doi: 10.1109/ECAI61503.2024.10607476.

L.7. ***"Experimental Analysis of Network Traffic Databases for Anomaly Detection"***

Autori: **Maria-Mădălina Andronache**, Alexandru Vulpe, Corneliu Burileanu

Anul publicării: 2023

Conferință: International Conference on Speech Technology and Human-Computer Dialogue (SpeD) 2023, Bucharest, Romania, **IEEEXplore;**

Stadiu: publicat, pp. 122-127, doi: 10.1109/SpeD59241.2023.10314928.

8.4 Perspective de dezvoltare ulterioară

Perspectivele de dezvoltare includ aplicarea noțiunilor pentru zona de cloud și implementarea suplimentară a unor caracteristici în cadrul mediului de test utilizat.

Bibliografie

[1] MalwareBazaar Database, https://bazaar.abuse.ch/sample/04789bb1e63b81997e53786d1f19a6dde477b29b54ad5bcb12aeb9bce3d0f72b/

[2] MalwareBazaar Database, https://bazaar.abuse.ch/sample/ef93353c2ecc677d4db0854d9eac80717a496af273ee0f2f5a21fda5682e248e/

...