NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY POLITEHNICA BUCHAREST

Doctoral School of Electronics, Telecommunications and Information Technology

Decision No. ____ from DD-MM-YYYY

Ph.D. THESIS SUMMARY

Maria Mădălina ANDRONACHE

TEHNICI DE ANALIZĂ A TRAFICULUI ÎN REȚELELE DE CALCUL

TRAFFIC ANALYSIS TECHNIQUES IN COMPUTER NETWORKS

THESIS COMMITTEE

Prof. Dr. Ing.	President
Prof. Dr. Ing. Corneliu BURILEANU	PhD Supervisor
Prof. Dr. Ing.	Referee
Prof. Dr. Ing.	Referee
Dr. Ing.	Referee

BUCHAREST 2025

Content

Chapter 1

Introduction

Information transported via the Internet has become one of the most important aspects of the 21st century. Basically, through this resource, the way in which people communicate with each other, have fun, work, shop, has changed. Thus, various activities that required additional time to perform have become much easier and more convenient.

In the current security context, network monitoring has become a necessity. Therefore, detecting security incidents or anomalies in a network becomes the main purpose served by appropriate monitoring.

Given the increasing intrusiveness of attacks and the fact that they can be extremely harmful, even if they may seem harmless, it is absolutely essential for security policies to be more restrictive and for user privileges not to be granted unnecessarily. In this paper, an overview of existing technologies that enable efficient network monitoring is presented, and the impact of new technologies such as IoT, SDN, and others is also taken into account.

1.1 Presentation of the field of the doctoral thesis

Cybersecurity, in the ever-expanding digital era, has become a critical aspect in protecting information technology resources (sensitive data, user privacy). Taking into account the continuous dependence on technology and the need for digitalization of all types of services and infrastructures, cyber threats have evolved a lot, both in terms of volume and in terms of methods of sophistication and masking of real intent.

These types of attacks do not only target ordinary users, but especially various organizations or institutions, numerous types of critical infrastructures, and countless technologies whose data is important.

The perpetrators of attacks are often malicious actors, but there are also situations where they group together, or they are hired by various states. Their goal is to detect various vulnerabilities and analyze various unsecured environments in order to steal information or cause major damage to a system.

Their methods include phishing techniques, malicious file attacks, and even DoS (Denial-of-Service) attacks.

In these circumstances, network traffic analysis plays a critical role in understanding how attacks or cyber threats work. Capturing, identifying, and testing

malicious code allows security administrators to determine the purpose, propagation methods, and detection evasion techniques used by attackers.

1.2 Scope of the doctoral thesis

The purpose of this work is to identify the best methods for capturing and analyzing network events. For this, several methods and techniques that led to increased efficiency were considered, both in terms of detection and prevention methods against such events.

These methods can extract indicators of compromise (IoC), build detection signatures, and develop response strategies tailored to each type of attack. In addition, the information obtained contributes to the continuous improvement of automated detection systems, the development of more effective security policies, and the training of incident response teams.

Thus, through traffic analysis methods, a strategic component of proactive defense can be built in a digital environment under constant pressure from emerging threats.

1.3 Content of the doctoral thesis

This paper presents 8 different chapters, which present various approaches to various methods of analyzing network traffic, both legitimate and malicious.

The structure of the paper includes several chapters, which will be detailed in the following paragraphs.

In Chapter 1, the introductory notions of the thesis and the field of cybersecurity were presented.

In Chapter 2, information on the current cybersecurity environment was presented, specifying related fields such as machine learning, static and dynamic analysis, but also Event Management and Security Information Systems.

In Chapter 3, current software solutions were identified and the benefits and limitations of each of them were analyzed, based on information from the literature.

Chapter 4 included the first set of effective analyses of the malware domain, using machine learning techniques and pre-labeled public databases, in order to identify the best intrusion detection algorithms.

In Chapter 5, the effective analysis continued through actual malicious files from the public resource area, which were analyzed through hybrid techniques (static and dynamic).

In Chapter 6, the analysis continued with experiments specific to network traffic event analysis, using various techniques based on SIEM systems.

Chapter 7 included the integration of the aforementioned methods at the level of a network infrastructure in the eve-ng simulated environment. Through it, various

attack scenarios and various methods of identifying them or protecting against them were generated.

In Chapter 8, the main conclusions, contributions of the work and perspectives for further development were introduced, along with the list of works published during the doctoral program.

Chapter 2

Computer network security

Network security is a set of policies, technologies and practices implemented to protect the integrity, confidentiality and availability of data and services in a communications infrastructure.

Essentially, network security aims to prevent unauthorized access to, or modification and destruction of, information transmitted over a network. Cyber threats are constant and complex and, thus, can lead to intrusions and theft of key information.

Therefore, network security involves a diverse set of mechanisms, including firewalls, intrusion detection and prevention systems (IDS/IPS), traffic segmentation and continuous monitoring, through SIEM solutions.

Moreover, if an attack is identified, it must be analyzed to understand the network vulnerabilities that led to its being allowed into the network.

Thus, network security is a dynamic process, which must be able to respond in real time to complex attacks.

2.1 Cybersecurity

Cybersecurity aims to protect information systems, networks, devices and data against digital attacks, unauthorized access, theft or damage.

In an ever-expanding digital environment, where almost all social, economic and governmental activities depend on technology, cybersecurity is becoming an essential component of the secure and stable functioning of society. The main goal of this concept is to ensure the confidentiality, integrity and availability of information, regardless of the form in which it circulates or is stored.

In a landscape marked by increasingly sophisticated attacks, cybersecurity is no longer an option, but a strategic necessity for protecting identity and infrastructure.

2.2 Machine learning

Machine learning techniques represent a set of methods by which computer systems can automatically learn certain characteristics of data and make decisions, based on the learned concepts, without being explicitly programmed for each situation.

Among the most widely used machine learning techniques are classification algorithms (Support Vector Machines, k-Nearest Neighbors or Naive Bayes), which are used to label data according to observable features.

In the context of cybersecurity in communication networks, these techniques are adapted for detecting anomalies, identifying malicious behaviors and automating the analysis process, providing a superior response capacity to emerging threats.

However, the performance of machine learning models depends on the quality and volume of data used for training, as well as on the appropriate selection of relevant features.

2.3 Static analysis and dynamic analysis

Static malware analysis refers to examining malicious code or files without executing them, with the aim of understanding their structure and intent in a controlled and secure manner.

This technique uses tools such as decompilers, string or function analyzers, to identify known signatures, suspicious code sequences or techniques to hide the real, malicious nature.

Dynamic analysis involves running malicious software in an isolated environment, such as a sandbox, to observe its behaviors: changes in system registries, network connections or actions on files.

This technique provides a detailed picture of the effects that malware can produce in a real system.

Combined, the two methods allow for a deeper and more precise understanding of computer threats: static analysis provides initial speed and efficiency, while dynamic analysis reveals hidden behaviors.

2.4 IDS/IPS type systems

The techniques implemented in IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) systems are designed to detect and, respectively, prevent suspicious or unauthorized activities in a network or computer system.

IDSs monitor traffic and events in the system, signaling possible intrusions, without directly intervening.

IPSs automatically block identified malicious traffic.

These systems use two main detection methods: signature-based detection, which compares observed activity to a database of known attacks, and anomaly-based detection, which signals deviations from normal system behavior.

2.5 SIEM systems

Security Information and Event Management (SIEM) systems are centralized security event monitoring and analysis solutions designed to provide real-time visibility into your IT infrastructure.

These systems collect, correlate, and analyze data from multiple sources, transforming large volumes of network events into useful information for threat detection and incident response.

An effective SIEM uses correlation rules, automated alerts, and behavioral analytics to identify suspicious activity.

In an increasingly complex cyber landscape, SIEM is becoming an essential component of security operations, enabling faster response to cyber-attacks.

2.6 Conclusions

In this chapter, the essential aspects of the field of cybersecurity and related fields have been identified. These have been presented, through several sections, for easier documentation of the key ideas necessary for understanding the experiments carried out in the paper.

Chapter 3

Intrusion analysis methods

Detecting malicious software or network intrusions involves identifying the presence or activity of malicious code in a computer system.

Network traffic analysis systems include several stages such as monitoring, detection, analysis and response.

Classic methods include signature-based detection, where suspicious files are compared to a database of known codes, and that which analyzes the structure and behavior of files, to identify suspicious characteristics.

In parallel, anomaly-based detection monitors the normal behavior of the system and signals deviations that may indicate malicious activities.

These classic methods are constantly improved with machine learning algorithms, capable of recognizing intrusions, in a much easier way.

Effective detection often involves a combination of static analysis, dynamic analysis and contextualization of behavior, in a broader security framework.

3.1 General network traffic analysis solutions

Network traffic analysis methods include event logs, which need to be analyzed.

However, to identify vulnerabilities in a network, it is necessary to analyze them using several tools. Some of these are:

1. Nmap and Nessus – which provide information about vulnerabilities, open ports and services.

2. Wireshark and tcpdump – which can analyze network packets to capture and inspect network traffic.

3. NetFlow Analyzer – which allows for analysis of network flows, to monitor performance and identify anomalies.

4. Suricata – which is an intrusion detection and prevention system (IDS/IPS) that analyzes network traffic in real time.

5. Snort – which is an open-source IDS/IPS system for detecting and preventing network attacks.

3.2 Machine Learning-based solutions

While machine learning technologies can bring a significant advantage in the rapid detection of attacks, their application in cybersecurity also poses significant challenges.

Tools and solutions for Machine Learning are:

1. WEKA – machine learning platform that includes algorithms for classification or regression.

2. Scikit-learn – machine learning library for Python, with algorithms for classification or regression.

3.3 Solutions based on static and dynamic analysis

Static analysis includes several key concepts such as signature inspection, metadata analysis or file structure verification.

Solutions used in this chapter are:

1. PEStudio – detects information about file structure and malicious imports used by executable files.

2. IDA Pro / Ghidra – decompiler-type solutions for file analysis at the assembly code level.

3. Strings – solution that extracts strings from binary files, useful for identifying indicators of compromise.

4. YARA – method that allows the definition of rules for identifying files with similar characteristics to an already known malicious file.

5. VirusTotal – database that aggregates results from dozens of antivirus engines and allows behavioral analysis.

Dynamic analysis involves running the malicious file, in an isolated environment, to identify its behavioral characteristics:

The solutions used in this analysis are:

1. Procmon – monitors system processes and activities in real time.

2. Wireshark – analyzes network traffic generated by malware to detect data exfiltration or connections to command and control (C2) servers.

3. Antivirus – solutions with automatic detections and advanced intrusive behavioral identification capabilities.

4. Strace – is a Linux system tool that can monitor the interactions of a file with the operating system

3.4 SIEM-based solutions

Security information and event management (SIEM) systems can collect data from various sources, with the aim of improving the detection of suspicious activity in the network.

SIEM solutions considered in this paper are:

1. OSSEC – open-source intrusion detection system with log analysis functionalities.

2. OSSIM – open-source platform that integrates multiple tools for collecting, correlating and analyzing network security data.

3. Wazuh – open-source security monitoring solution that extends the capabilities of OSSEC, adding advanced analysis functionalities, intrusion detection and incident management in a distributed environment.

3.5 Conclusions

This chapter analyzes the main existing solutions for intrusion analysis. Thus, they were analyzed comparatively, identifying, through literature, the advantages and disadvantages of each solution.

Chapter 4

Detecting anomalies within a network using machine learning techniques

In cybersecurity, machine learning plays a critical role due to its ability to identify complex patterns and detect and respond to threats faster than traditional methods. It allows security solutions to continuously adapt to new types of threats, thereby improving prevention and response to cyber incidents.

4.1 How to use machine learning techniques for anomaly detection

Using machine learning in malware detection involves training models that can learn to distinguish between malicious and legitimate files or behaviors, based on features extracted from the input data.

The process begins by collecting a large set of labeled data, which includes malware and non-malware files, and extracting relevant features.

Machine learning models are trained on these features to learn the patterns associated with each file type.

After training, the model can classify new files or be evaluated using predefined performance metrics.

4.2 Identifying traffic anomalies using WEKA

WEKA is a widely used platform for applications involving machine learning, having implemented a wide range of different classification algorithms.

In this chapter, a public database is used, which is tested using several different algorithms, as shown in Figure 4.1.

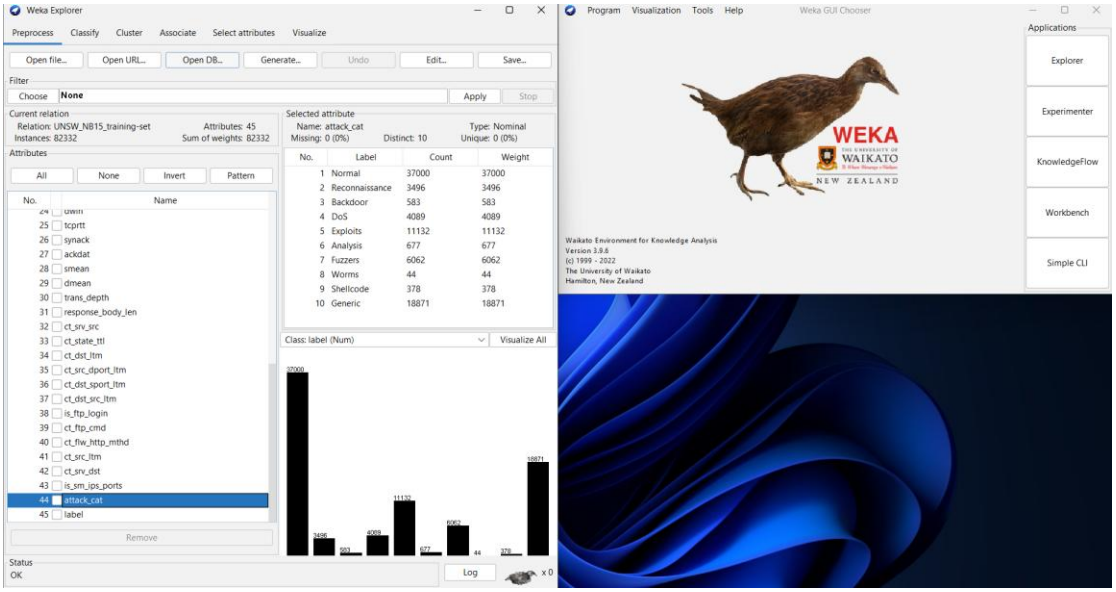

Figure 4. 1: *Loading the database into the WEKA solution*

4.3 Identifying traffic anomalies using Scikit-learn

Scikit-learn is a software solution that includes a collection of libraries that can implement machine learning algorithms.

In this chapter, the same database is used as in the previous case, which is tested through a Python program that also includes Scikit-learn libraries. The way in which the functions are implemented in this chapter is shown in Figure 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)
```

Figure 4. 2*: Test method used in Python with Scikit-learn*

4.4 Comparative analysis of the results obtained through the two solutions

The comparative analysis carried out in this chapter includes a multitude of performance parameters, data partitioning methods and machine learning algorithms, similar to the representation in Figure 4.9.

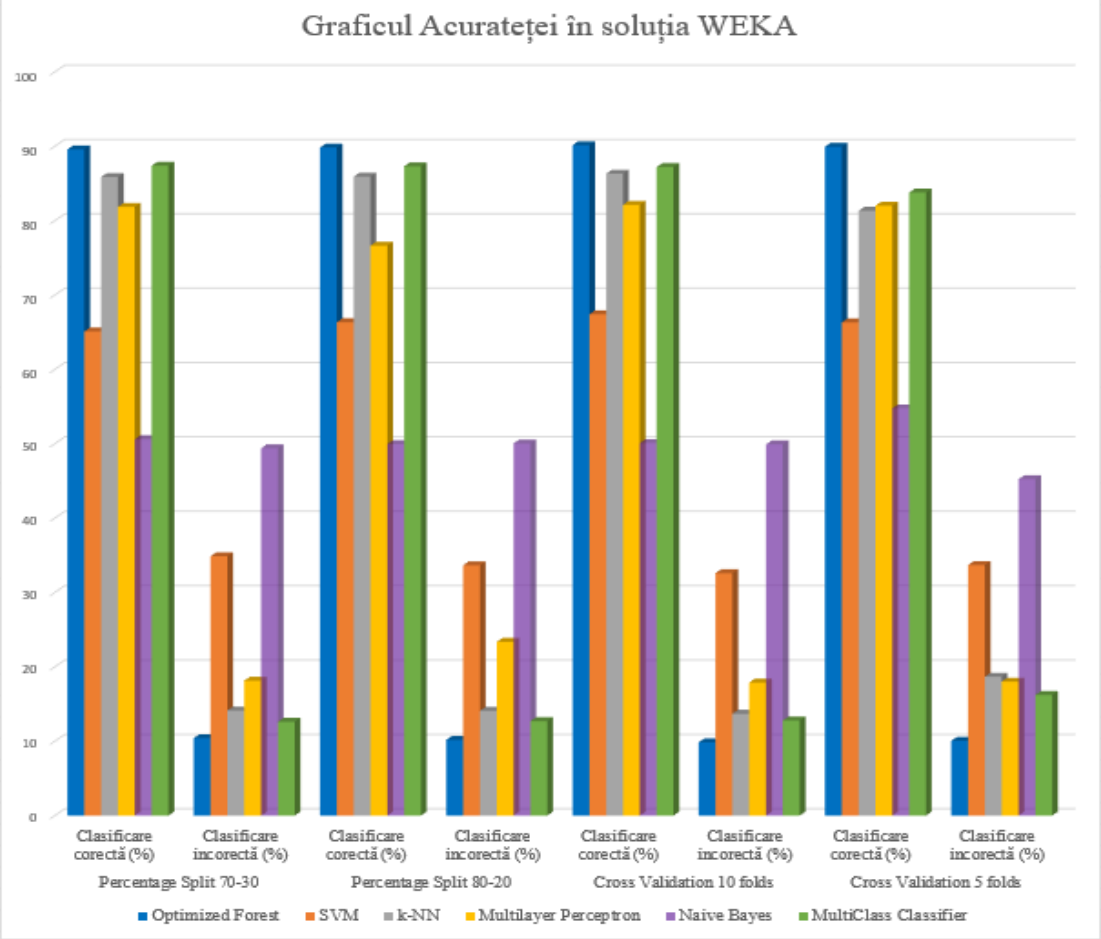

***Figure 4. 3**: Accuracy parameter graph within the WEKA solution*

4.5 Conclusions and original contributions

In this chapter, the two solutions which implement machine learning concepts, were comparatively analyzed.

The essential original contribution was that, during the chapter, most of the information classification algorithms for the used data set were identified and a comparative analysis of them was performed, taking into account several performance indices.

Chapter 5

Detection of the characteristics of a malicious file within a network, through static and dynamic analysis methods

Hybrid analytics in cybersecurity combines static and dynamic analytics approaches, creating a more robust and efficient system. By integrating these solutions, more accurate results and better incident management can be achieved, providing data that can lead to comprehensive protection and faster response to attacks.

5.1 Malicious files used in static and dynamic analysis

The malicious files in this chapter are characteristic of the Internet resource area and include samples such as those in Table 5.1.

Adware	**A1**	04789bb1e63b81997e53786d1f19a6dde477b29b54a d5bcb12aeb9bce3d0f72b [1]
Malware	**M1**	ef93353c2ecc677d4db0854d9eac80717a496af273ee0 f2f5a21fda5682e248e [2]

Table 5. 1: *Malicious files analyzed*

5.2 Using static analysis for anomaly detection

Examining files through this analysis includes several stages such as collecting information, identifying key concepts, and decomposing the code.

All these stages are analyzed and detailed in this chapter, with the aim of identifying a coherent way of working for carrying out experiments.

5.3 Identifying malicious characteristics of a file through static analysis

Within the experimental data, the files are analyzed using several tools, which identify various types of features such as those in Figure 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

***Figure 5. 1**: How the S1 malware file is analyzed using PEStudio*

5.4 Using dynamic analysis for anomaly detection

Dynamic analysis includes, from an experimental point of view, performing steps such as configuring the test environment, analyzing the interaction of the malicious file with various system aspects, and identifying the behavioral characteristics associated with these interactions.

All these steps are analyzed and detailed in this chapter, with the aim of identifying a coherent way of working for carrying out the experiments.

5.5 Identifying malicious characteristics of a file through dynamic analysis

Within the experimental data, the files are analyzed using several tools, which identify various types of features such as those in Figure 5.11.

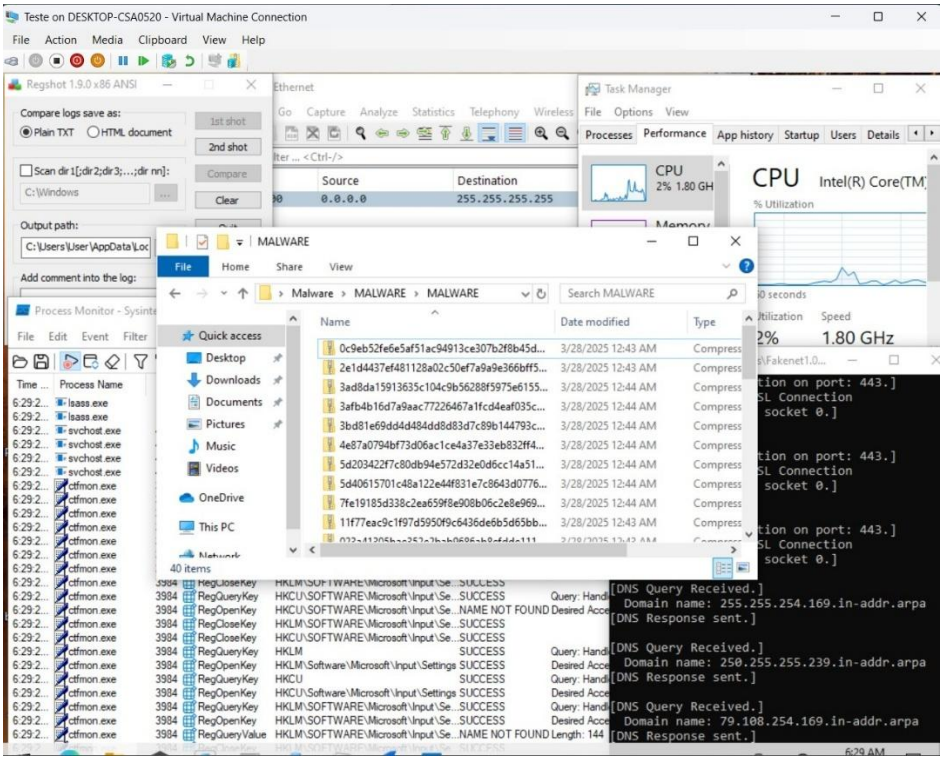

Figure 5. 11: *How to perform dynamic analysis, along with the tools and samples used*

5.6 Conclusions and original contributions

In this chapter, several types of malicious files were analyzed. Their functionality was tested both through static analysis, without executing the file, and through dynamic analysis, with its execution in a controlled environment.

The key original contribution was given by the identification of malicious characteristics based on several complementary solutions and their analysis, from a comparative point of view, in order to perform a more complete characterization of a certain type or family of malware.

Chapter 6

Detection of malicious traffic or programs within a network, through SIEM systems

SIEM (Security Information and Event Management) systems are used in malware detection by centralizing, correlating, and analyzing in real time data generated by different components of the IT infrastructure. It collects security logs and alerts, correlates them, and analyzes them to identify suspicious activities associated with the presence of malware. Through these methods, a SIEM allows security teams to quickly detect malware attacks, investigate their context, and respond effectively to limit the impact on the organization.

6.1 Using the OSSEC SIEM solution

The OSSEC system is a SIEM solution that works on the Agent-Manager principle, collecting logs from multiple sources and integrating them, centrally, for subsequent analysis.

The advantages of OSSEC are that it is an open-source system and that it can be considered a technological environment conducive to learning.

The disadvantages of this solution include platform instability, frequent agent disconnections, and a graphical interface that frequently interrupts.

Throughout the chapter, other advantages and limitations of the solution were also analyzed.

6.2 Using the OSSIM SIEM solution

OSSIM, developed and supported by AlienVault, is one of the most mature open-source solutions in the field of cybersecurity, offering an integrated framework for event collection, correlation and analysis.

Another major advantage of the solution is the graphical interface because it allows multiple ways of viewing alerts and even dynamic graphs.

One of the main disadvantages concluded through experiments was the rather high complexity of the OSSIM system in the installation area.

Throughout the chapter, other advantages and limitations of the solution were analyzed.

6.3 Using the WAZUH SIEM solution

Wazuh is a SIEM solution derived from OSSEC but significantly improved in terms of functionalities.

An advantage of this solution comes from the fact that it is very versatile in terms of recording logs from various network equipment or even various types of applications.

A disadvantage is the high consumption of resources required for installation and initial configuration.

Throughout the chapter, other advantages and limitations of the solution were analyzed.

6.4 Comparative analysis of the performance of the analyzed SIEM systems

Following the comparative analysis of the SIEM methods used, the advantages and disadvantages were identified experimentally visualized.

According to this, a hierarchy of the performances of each system was also created.

6.5 Conclusions and original contributions

The conclusions of this chapter consisted in identifying the most suitable SIEM system for monitoring and characterizing events within a network.

The main original contribution was made by the comparative testing of these solutions and the identification of the limitations and advantages of each solution, in part.

Chapter 7

Detection of anomalies or malicious files within regular network traffic

Constant monitoring of network events leads, implicitly, to an efficient detection of anomalies recorded at their level.

The process of detecting them includes certain stages that are based on advanced data analysis or machine learning techniques such as:

1. Network data collection
2. Creation of normal traffic models
3. Anomaly detection

7.1 Network architecture

To create efficient test scenarios, a complex network architecture was created, which can be found in Figure 7.1.

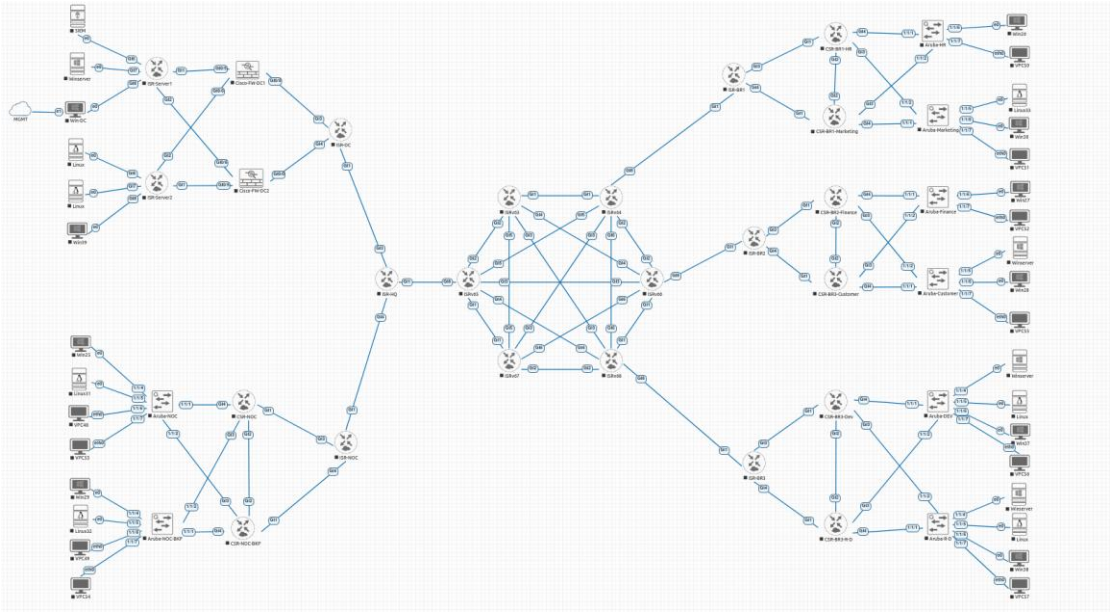

***Figure 7. 1**: General architecture of the analyzed network*

7.2 Simulating network-level cyber attacks

The most likely attacks at the network level are network scans, network flooding attacks, or denial of service (DoS) attacks.

All of these are experimentally represented through this chapter.

7.3 Simulating cyber-attacks via malicious files

In this chapter, also through the eve-ng virtualized environment, a realistic scenario was created in which infections with malicious files were simulated, which are masked in legitimate files, and which are executed on the network.

The simulations included the execution of several types of malicious files such as ransomware, spyware, malware, etc.

7.4 Static analysis of malicious files used

In this chapter, all previously executed file types were analyzed, both for the Ubuntu operating system area and for the Linux operating system area.

In this way, the main characteristics of each file type were extracted, in part.

7.5 Analysis of malicious files through Machine Learning techniques

In the context of the network architecture used, WEKA-type solutions or integration of processes with Scikit-learn libraries is done to correlate various events and to learn various patterns of normal behavior.

This way of working involves exporting traffic files from the SIEM system, cleaning them and introducing them into machine learning solutions for analysis.

7.6 Network traffic analysis mode

Throughout this chapter, but also throughout this paper, several ways of analyzing network traffic were presented, with the aim of detecting various intrusions and finding the most appropriate security solutions for a real network environment.

7.7 Conclusions and original contributions

In this chapter, a proprietary network infrastructure was created, which also included various traffic analysis methods. Also, through the proposed network architecture, various attacks or executions of malicious files were simulated, whose characteristics and behavior were analyzed, using all the techniques mentioned in the previous chapters.

The major contribution consists in the creation of the test environment and the comparative analysis of the intrusions.

Conclusions

The present work used several network traffic analysis techniques and can be a solid basis for carrying out concrete and accurate research analysis of the security field, on different levels of intrusion.

8.1 Obtained results

The results obtained are schematically presented as follows:

1. In the First Chapter, the key aspects of the work were made aware.
2. In Chapter 2, the theoretical aspects and their essential notions were presented.
3. From Chapter 3, the understanding of the functioning of the technologies used in the field of cybersecurity resulted.
4. In Chapter 4, the result consisted in the identification of ideal machine learning algorithms for intrusion detection.
5. From Chapter 5, the understanding of the key characteristics in the functioning of a malicious file resulted.
6. At the level of Chapter 6, the functioning of network intrusions, captured through a SIEM system, was identified.
7. In Chapter 7, all previous analysis methods for the detection of intrusions within a proprietary network architecture were introduced.

8.2 Original contributions

The original contributions of this work were obtained both through the documentation area on the current cybersecurity context, and through the implementation in real or simulated environments of various test scenarios, to obtain experimental results.

All of these can be divided as follows:

1. Comparative analysis of open-source solutions and identification of those to be tested at the experimental level.

2. Carrying out experiments based on Machine-Learning solutions, using WEKA and the Python programming language, through which various functions and libraries from the Scikit-learn area were implemented. These experiments were multiple, using various testing methods and various analysis parameters

and performance indices, with the aim of defining a hierarchy of the best algorithms for classifying data sets that also contained intrusions.

Articles: 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. Implementation of architecture based on a virtual environment, which can include the analysis of open-source solutions and the inclusion of an IDE (Integrated development environment), through which experiments including Machine-Learning can be carried out, in the Python programming language.

4. Performing a hybrid static and dynamic analysis on several different types of malicious files, highlighting their key impact aspects, in Linux and Windows operating systems. Also, their defining aspects were extracted and comparatively analyzed, both from a structural and experimental point of view, in order to be able to make a complete characterization of how they can infect a computer network.

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

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

5. Testing various static and dynamic analysis solutions, both from a comparative point of view and from the point of view of identifying as much key information as possible that can define certain malicious files.

6. Implementation of a virtual environment-based architecture, which includes static and dynamic analysis of solutions. Therefore, isolated environments were created, which would influence the production environment as little as possible, but which could simulate a real environment.

7. Implementation of a network architecture, which included several virtual machines whose network logs were monitored through an agent-manager SIEM solution. Through this architecture, various types of attacks were tested, which were monitored and displayed through a graphical interface. All of these included both the Windows operating system and the Linux operating system.

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

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

8. Testing various SIEM solutions from a comparative point of view, to identify the best way to monitor network events and to identify their various advantages and disadvantages.

9. Implementation of a proprietary network architecture, which included both network equipment configuration elements and different ways of resource communication. These were included in an eve-ng type environment, respecting the principles of segmentation and differentiated access to various types of resources.

10. Based on the previously created network architecture, Security Event and Information Management solutions were included, various attack scenarios were created, using common network attacks and network attacks based on various types of malicious files. All these intrusions were subsequently analyzed within the same network, in order to define their defining characteristics.

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

11. Through the network architecture, various malicious files were analyzed, from a static and dynamic point of view, and ways of implementing machine learning solutions were also identified, which could be included in the test environment.

12. Throughout the work, various intrusion protection measures were defined and implemented, resulting from the experiments carried out.

These contributions can influence awareness of the complexity of the cybersecurity environment and can lead to the optimization of certain processes and methods directly involved in it.

8.3 List of original publications

During the research activity during the doctoral internship, the author published a number of 7 scientific papers related to the field of the doctoral thesis, of which 7 as first author and 4 indexed in IEEEXplore:

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

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

Year of publication: 2025

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

Stadium: accepted, in process of publication

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

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

Year of publication: 2025

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

Stadium: published, pp. 000065-000070, doi: 10.1109/SAMI63904.2025.10883178.

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

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

Year of publication: 2024

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

Stadium: published, doi: 10.14569/IJACSA.2024.0151257

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

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

Year of publication: 2024

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

Stadium: published, 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"***

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

Year of publication: 2024

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

Stadium: published, pp. 1-6, doi: 10.1109/COMM62355.2024.10741424.

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

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

Year of publication: 2024

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

Stadium: published, pp. 1-6, doi: 10.1109/ECAI61503.2024.10607476.

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

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

Year of publication: 2023

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

Stadium: published, pp. 122-127, doi: 10.1109/SpeD59241.2023.10314928.

8.4 Perspectives for further developments

Development prospects include applying the concepts to the cloud area and further implementing some features within the test environment used.

Bibliography

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

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

...