ISSN No:-2456-2165

Extended Model of Isolations and Boxing on Main Frame Computer Network Security Counter Measures Based on Big Data

(Topic Area: Network security)

Pascal HABUMUGISHA Master's, Dr. Musoni Wilson PhD,
Master of Science in Information Technology (MSCIT), University of Kigali, Rwanda

Abstract:- The controls employed to safeguard the availability, confidentiality, and integrity of data and information systems are known as security countermeasures. At every level of the stack, a vast range of security controls are accessible. It is essential to prevent malicious damage while information is carried over a network. Additional security measures, the removal of unnecessary services, hardening systems, and access control can all significantly improve overall security. Therefore, sandbox systems are essential to the secure operation of countermeasures against network security. Networked information is susceptible to a wide range of assaults. In this paper, we suggested an isolation table for hierarchical networks to identify intrusions and estimate the impact of intrusion detection.

The main experiment shows that sandboxing is a useful tool for preventing attacks. The goal of this study was to compare intrusion detection and prevention systems (IDS/IPS) with sandboxes in computer network security. The primary goals of this study are to examine the value of sandboxing computer network security countermeasures in comparison to identification and prevention systems (IDS/IPS) and to examine the procedures that need to be followed in order to launch different types of active and passive assaults on the network. harmful attacks are bad for the Network and for anyone that use the Internet without enough security. We need to put in place trustworthy security. for a variety of uses.

The qualitative method of primary research will be used to obtain the research study's outcomes. The targeted sample population (IT) is to be interviewed in an open-ended manner, providing them with an opportunity to fully express their perspectives regarding the study problem and the questions posed. Additionally, the study's sample population included NISR IT personnel. Both primary and secondary data were used; primary data were gathered through questionnaires, and secondary data came from pre-existing datasets. R Data Analytics, Manage Engine Analytics Plus, NMAP, Advanced IP Scanner, Wireshark, and Kali Linux for penetration testing algorithms will be utilized for model analysis. Analyzing performance model methodologies is the goal of this study.

Keywords:- *Sandbox, NMPA, kali Linux, IP Scanner, Big Data, Wire Shark.*

I. INTRODUCTION

By offering a regulated, segregated environment for executing applications and doing data analysis, sandboxing can enhance big data security. With the help of sandboxes, developers, security teams, and data scientists may test and operate big data apps in a safe setting without exposing confidential information or introducing dangerous code. Additionally, sandboxing can provide an additional degree of security when handling data from dubious sources, such the internet. But the quality of the implementation, the application of suitable security measures, and the environment's continual monitoring to identify and address security threats all affect how effective sandboxing for big data security is. Sandboxing is generally a good security tool.

We have now reached the Big Data Era thanks to the widespread proliferation of the internet, internet of things, and cloud computing technologies. Businesses can increase their production capacity and strengthen their own advantages by utilizing effective big data technologies. But a number of possible catastrophes also come after. Data leaks are turning into a major information security disaster for multinational corporations.

Data leaks cause enterprises' credibility to decline and often result in significant property losses. Thus, in the Big Data Era, It's More Important Than Ever to Learn How to Prevent in Advance A sandbox is a security measure used to isolate running processes in an attempt to prevent software vulnerabilities and/or system failures from propagating. Using the sandboxing technique, you establish a separate testing environment.

II. METHODOLOGY

- **Data analysis:** R analytics is the process of analyzing data using the R programming language, an open-source tool for statistical computing and visuals.

ISSN No:-2456-2165

R's business analytics facilitates more effective firm data analysis for users. Some of the biggest benefits that businesses using R in their analytics initiatives have experienced are as follows:

- **Democratizing Analytics Throughout the Organization:** R can contribute to the democratization of analytics by providing interactive reporting and data visualization capabilities for business users. R may be used by non-data scientists to undertake data science, enabling citizen data scientists and business users to make better informed decisions. Additionally, R analytics can free up data scientists' time so they can work on more complex data science projects by reducing the amount of time they spend preparing and organizing data.
- **Leveraging Big Data:** Several business leaders use R, a programming language that allows for large-scale data queries, to leverage big data across their enterprises. R analytics can help businesses make sense of their enormous data sets and find fresh insights. Large datasets like this can be handled by R, and for the majority of analysts, it's probably just as simple to use as, if not simpler than, any other analytics program available today.
- **Making Interactive Data Visualizations:** R is helpful for data visualization and data exploration since it makes the creation of graphs and diagrams easier. It offers the capacity to Provide 3D charts and graphs, together with interactive visualizations, so that business users may interact with them.
- **Manage Engine Analytics Plus:** With automated insights, Analytics Plus integrates IT data from several applications and monitoring technologies to help you make strategic decisions more quickly. Analytics Plus assists you in achieving excellence in all areas of IT, including compliance, costs, and tickets pertaining to SLAs, security, and technician performance.
- **Wireshark:** Wireshark is a packet analyzer for networks. A network packet analyzer displays captured packetdata as preciselyas possible.

Consider a network packet analyzer to be a measuring device for examining what's going on insidea network cable, similar to how an electrician uses a voltmeter to examine what's going on inside an electric cable(but at a higher level, ofcourse).

Previously, such tools were either prohibitively expensive, proprietary, or both. That has changed with the introduction of Wire shark. Wire shark is a free, open source packet analyzer that is one of the best available today.

- **NMAP:** A free and open source tool for network discovery and security auditing is called Nmap (Network Mapper). It is widely used by system and network administrators for activities such as managing service update schedules, keeping an eye on host or service uptime, and inventorying networks. Nmap uses cutting-edge methods to find hosts on the network, the services (name and version of the application) those hosts offer, the operating systems (and OS versions) those hosts are running, the kind of packet filters/firewalls those hosts are using, and a host's many other features. Although it was intended to scan vast networks rapidly, it is also effective on single hosts. Nmap provides official binary packages for Linux, Windows, and Mac OS X and is compatible with all major computer operating systems.

- **Kalilinux:** A free and open-source Linux system called Kali Linux is designed for information security jobs like reverse engineering, computer forensics, penetration testing, and security research.
- **Distribution of respondents by Title:** It was requested of the responders to identify their title. To ascertain whether the respondents had taken part in Sandbox System security, information about their title was obtained. The table 1 below provides an overview of the responses.

Table 1: Distribution of respondents by Title

Position	Frequency	Percentage
NISRStaffIT	267	88.4
Staff	35	11.6
Total	**302**	**100**

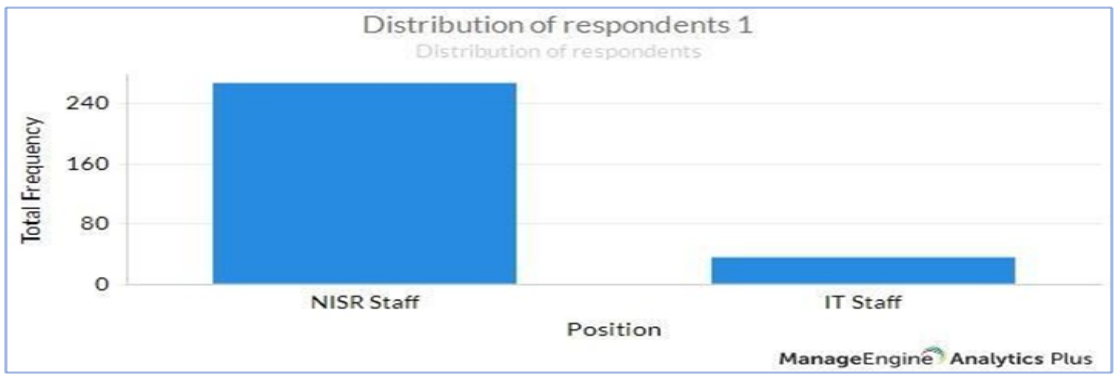

Fig. 1: Respondents

III. SECURITYTECHNOLOGIESINNATIONALINSTITUTEOFSTATISTICINRWANDA

Additionally, the respondents were asked to list the security technology that NSIR currently uses. Security technologies play a critical role in this study because they shield sensitive data from illegal access, data breaches, and other disruptive security risks that affect consumer and company data.

Table 2: The Security Technologies in NISR

Security Technologies	Frequency	Percentage
Sandbox	0	0
Firewall	158	52.3
Network Access Control Virtual	0	0
Private Network(VPN)	80	26.4
Intrusion Detection Systems/Intrusion Prevention System	19	6.2
Others or Unknown	45	14.9
Total	**302**	**100**

IV. RATEOF SECURITYOFBIGDATAINNISR

Additionally, the respondents were asked to rank the information system's security within NISR. Because it protects sensitive data from cyberattacks and guarantees that the network is reliable and useable, security rate is crucial in this study.

Table 3: Rate of Network Security

Rate of Network Security	Frequency	Percentage
Very secure	146	48.3
Secure Unsecure	81	26.8
Very	53	17.2
unsecure	22	7.2
Total	**302**	**100**

V. EXTENDEDS AND BOX FLOW CHART

Beyond just describing the purpose, user actions, data flow, security measures, monitoring, error handling, collaboration, documentation, testing, maintenance, and contingency plans within the environment, an extended sandbox flow chart is a visual representation of the processes and interactions within a sandbox environment. It offers a thorough understanding of how the sandbox functions and is kept up to date, assisting in ensuring both its security and functionality.

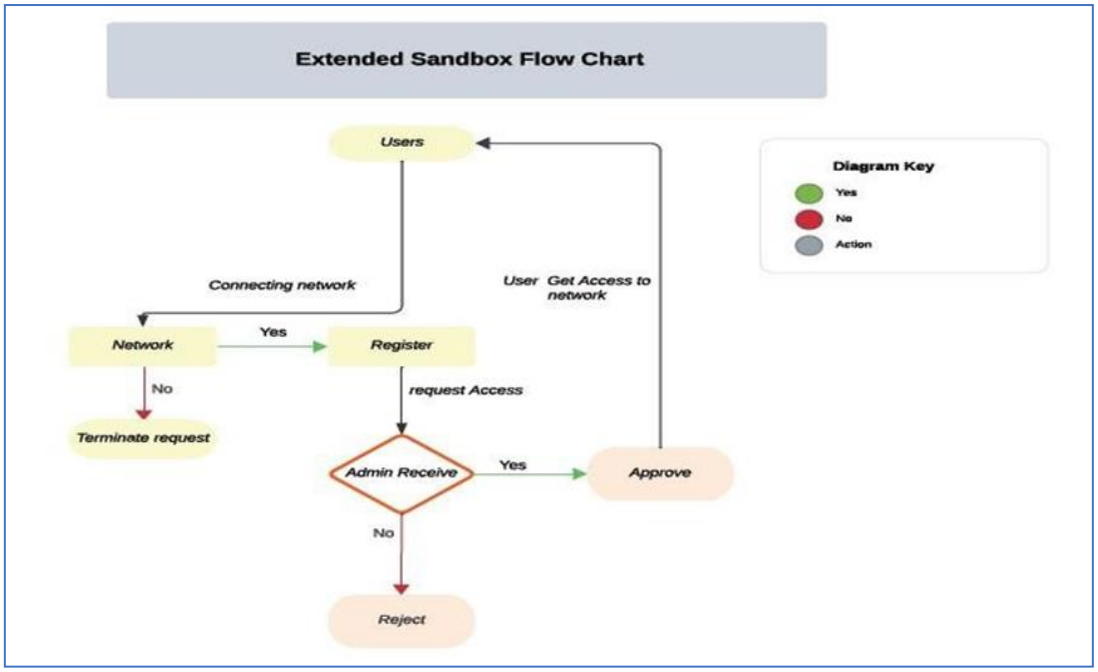

Fig. 2: Extended Sandbox Flow Chart

VI. SUMMARY OF ASSESSMENT

The diagrambe low summarizes the gaps identified in software/hardware/too ls during the assessment of the NISR network security 5 layers in network security infrastructure:

A. Data Layer

This layer describes the inspection of data packets to detect attempts to compromise network applications.

B. End Point Layer

This layer focuses on technologies that protect the IT environment through keeping track of activities, authorization and authentication of client /server devices (end point devices).

C. Network Layer

This layer contains technologies that restrict and control access to critical network assets

D. Perimeter Layer

This refers to software/hardware/tools that protect the boundary between the private and locally managed-and-owned side of a network and its public, usually provider-managed side.

E. Security and Monitoring Layer

The software/hardware/tools in this layer aid in keeping watch against threats to the ITenvironment.An alert is raised whenever asuspicious activity is detected.

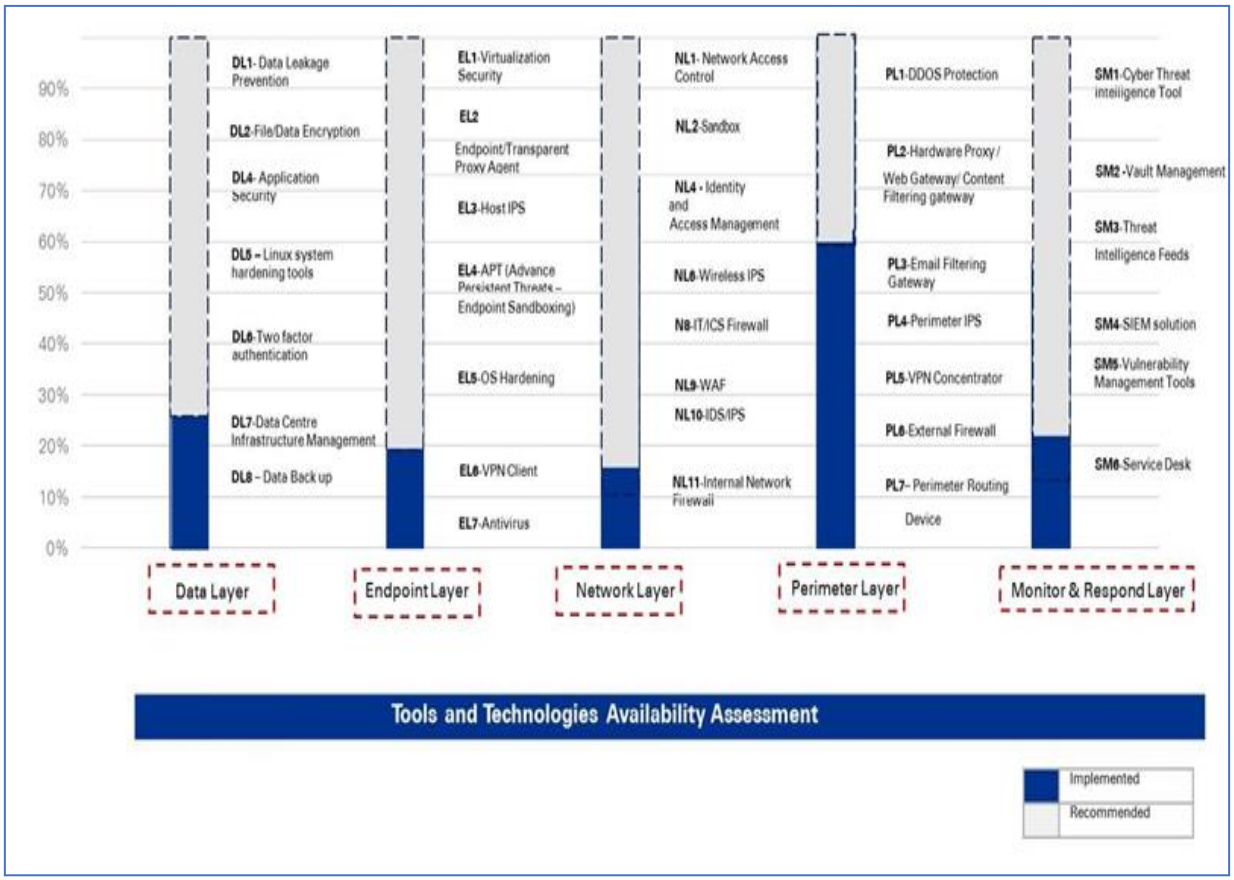

Fig. 3: Penetration Testing Finds

VII. CONCLUSIONS OF THE STUDY

In its IT infrastructure, NISR has deployed a variety of hardware, software, and applications, including VPNs, e-learning, email gateways, data backup solutions, and service desks.

Most of the tools, hardware, and software available for the perimeter layer have been deployed by NISR. However, in order to strengthen the network security posture of NISR due to Sandbox isolation, essential software, hardware, and tools must be implemented across all tiers.

REFERENCES

[1]. Asiamah, N.(2017). *General, Target and Accessible Population: Demystifying the Concepts for Effective Sampling*. Qualitative research conference.
[2]. Buzan, B.(1991). *New Patterns of Global Security in the Twenty-First Century*. Oxford University Press.
[3]. Chen, X. (2017). *Big Data Analytics for Network Security and Intelligence.*
[4]. Engineering, R.C.(2020). *Ssecurity Infrastructure.* AICTE.
[5]. Fessant, F.L.(2011). *A Sinkhole Resilient Protocol for Wireless Sensor Networks: Performance and Security Analysis.* Published by Elsevier.

[6]. Fisler, K.(2011). *Major Shortage of Cyber Security Work force Professionals.* The ACM Guide to Computing Literature.
[7]. Francis.(2019). Research on the Integration of Internet. *Rancis Academic Press*.
[8]. Golafshani, N.(2003). *Understanding Reliability and Validity in Qualitative Research.* Open Journalof Business and Management.
[9]. Jordan, C. (2011). *Counter Measures game for teaching computer security.* IEEE.juvva,k.(1997).*a resource-centric approach in real time and multi media system.*
[10]. Kaur,B.(2018). *Cloud-Based Intrusion Detection and Response System Open.* Group of ESRG journals.
[11]. Kvale,S.(2007). *Doing Interviews.* SAGE Publications Ltd.
[12]. Leganza, G.(2015). *ANNUAL REPORT PURSUANTTO SECTION 13 OR 15(d)OF THE*
[13]. *SECURITIES EXCHANGE ACT.* Forrester Research, Inc.
[14]. Mc Combes, S.(2019). *Sampling Methods|Types, Techniques & Examples.* Shona Mc Combes.
[15]. Miwa, S.(2007). Design and implementation of an isolateds and box with mimetic internet used to analyze malwares. all Oino,D. I. (2018).*Leadership Stylesand JobSatisfaction.*
[16]. Orodho,J.(2009). *ELEMENTS OF EDUCATION AND SOCIAL SCIENCE RESEARC.* NAIROBIKANEZJA.
[17]. PhD, J. R. (2017). *Pedagogy, Leadership, and Leadership Development.*
[18]. https://doi.org/10.1002/pfi.21734.
[19]. Prensky, M.(2003). *Digital Game-Based Learning," ACM Computers in Entertainment.*
[20]. Association for Computing Machinery.
[21]. Rojas, J. A. (2017). *Sampling Techniques toImprove Big Data Exploration.* IEEE through Carnegie Mellon University, School of Computer Science, Pittsburgh PA, US.
[22]. S.F.Rossouw.(2000).*ResearchMethodologyfortheBusinessandAdministrativeSciences.* AOSIS(Pty)Ltd.
[23]. S.F.Rossouw.(2017).*Research Methodology for the Business and Administrative Sciences.*
[24]. AOSIS Open Journals.
[25]. Sachan, R.S.(2013). *A cluster based intrusion detection and prevention technique for mis direction attack inside WSN.* India: International Conference on Communication and Signal Processing.
[26]. Sachan,R.S.(2013).*Aclusterbasedintrusiondetectionand preventiontechniqueformisdirectionattackinsideWSN.*IEEE.
[27]. Sandbox,K. (n.d.).KasperskySandboxUsabilityHowitworks.SvendBrinkmann, S. K. (2018). *Doing Interviews.*
[28]. Yuqing,L.(2017).*ResearchonPersonalInformation Security on Social Networkin Big Data.*IEEE.