FMDB *Transactions on Sustainable Computer Letters*

In-Depth Analysis and Implementation of Advanced Information Gathering Tools for Cybersecurity Enhancement

J. Angelin Jeba[1,*], S. Rubin Bose[2], R. Regin[3], S. Suman Rajest[4], Utku Kose[5]

[1]Department of Electronics and Communication Engineering, CEG Campus, Anna University, Chennai, Tamil Nadu, India.
[2]Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[3]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[4]Department of Research and Development & International Student Affairs, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
[5]Department of Computer Engineering, Suleyman Demirel University, Kazakhstan, Turkey.
jebaangelin@gmail.com[1], rubinbos@srmist.edu.in[2], regin12006@yahoo.co.in[3], sumanrajest414@gmail.com[4], utkukose@sdu.edu.tr[5]

Abstract: Information gathering constitutes a foundational phase in cybersecurity, representing the initial reconnaissance stage where critical data on target systems, networks, and organizations is systematically acquired. This abstract examines the pivotal facets of information-gathering tools within the cybersecurity domain. These tools are integral to ethical hacking, penetration testing, and vulnerability assessment, facilitating security professionals in comprehending vulnerabilities, appraising risk, and bolstering defensive mechanisms. The diverse categories of information-gathering tools encompass network scanners, vulnerability scanners, DNS enumeration tools, web application scanners, social engineering tools, and open-source intelligence (OSINT) tools. Each tool category serves a specific function in the information-gathering process, spanning the identification of live hosts and open ports, assessing web application vulnerabilities, and extracting publicly available data on targets. The ethical dimension is paramount in deploying information-gathering tools, necessitating strict adherence to legal and ethical frameworks and obtaining proper authorization before initiating any scanning or probing activities.

Keywords: Information Gathering Tools; Cybersecurity Enhancement; Ethical and Regulatory Challenges; Evolving Threat Landscape; Managing Large Volumes of Data; Systems Information Spread Challenges; Dynamic Network Analysis Challenges.

Received on: 16/01/2023, **Revised on:** 26/03/2023, **Accepted on:** 03/05/2023, **Published on:** 05/06/2023

Cited by: J. A. Jeba, S. R. Bose, R. Regin, S. S. Rajest, and U. Kose, "In-Depth Analysis and Implementation of Advanced Information Gathering Tools for Cybersecurity Enhancement," FMDB Transactions on Sustainable Computer Letters., vol. 1, no. 2, pp. 130 –146, 2023.

1. Introduction

The landscape of open sources, an enduring domain, has undergone a transformative evolution with the advent of the Internet and the World Wide Web (WWW). This transformation has captivated the attention of cybersecurity professionals and motivated researchers to delve into cyber threats, cyber-criminal profiling, and information gathering, as underscored by Amaro et al. in their 2018 work [16]. At the intersection of this evolution lies the amalgamation of Artificial Intelligence (AI) and Machine Learning (ML) analysis, posing a nuanced challenge for practitioners in the domain of open-source intelligence

[*]Corresponding author.

(OSINT) [17]. The focal point is on harnessing the potency of publicly available unstructured data to fortify cybercrime investigations, necessitating the development of sophisticated methodologies for identification, collection, and organization [18].

The term "OS" in OSINT aptly denotes "Open Source," signifying publicly accessible repositories from which users derive information for intelligence [19]. Here, the term "Information" emerges as a pivotal component of OSINT, embodying freely available data that doesn't necessitate the skillset of a hacker to access. Individuals may have unwittingly employed OSINT tactics in their daily lives, perhaps during an online search for a company, school, university, or individual. The omnipresence of OSINT transcends storage locations or mediums, be it social networks, photographs, videos, blogs, newspapers, or tweets. The only requisite is that the information is public, accessible, and obtained legitimately [20]. In essence, OSINT becomes a democratizing force, rendering valuable intelligence accessible to a broader audience, extending beyond the purview of cybersecurity professionals [21]. Leveraging a profound understanding of OSINT principles can confer significant competitive advantages. One such advantage is the ability to profile criminals with a depth and granularity that traditional investigative methods may find challenging [22]. OSINT equips investigators with the tools to traverse the digital landscape, tracking employees of companies and unearthing connections that might elude conventional scrutiny. Moreover, OSINT becomes a potent instrument against organized crime, enabling law enforcement agencies to follow digital trails, connect the dots, and stay one step ahead of criminal networks [23].

However, integrating AI and ML into the OSINT framework introduces a layer of intricacy. The vastness and diversity of open-source data necessitate sophisticated algorithms and models to distill meaningful insights. Researchers are actively devising methodologies that can navigate this uncharted terrain effectively [24]. The challenge lies in the sheer volume of data and the dynamic nature of the online environment. New sources emerge, and the digital landscape evolves, demanding adaptive and resilient analytical frameworks [25]. Furthermore, the ethical considerations surrounding OSINT cannot be overstated. The power to access and analyze public information brings a responsibility to uphold privacy and adhere to legal boundaries. Striking the right balance between extracting actionable intelligence and respecting individual privacy is an ongoing challenge. The ethical use of OSINT requires obtaining information through lawful means and ensuring that the methods employed align with established legal and ethical norms [26].

The confluence of open sources, AI, and ML presents a dynamic landscape for cybersecurity professionals and researchers. OSINT, as a discipline, emerges as a potent tool in the digital age, democratizing access to intelligence and empowering individuals beyond the traditional realms of cybersecurity [27]. While challenges abound, from integrating AI into OSINT practices to the ethical considerations inherent in information gathering, the potential benefits, including enhanced criminal profiling and advanced investigative capabilities, underscore the importance of continued exploration and refinement of OSINT methodologies. As technology continues to evolve, so must our approaches to harnessing the vast sea of open-source information for the greater good of digital security and intelligence [28].

.

2. Literature Review

Yadav et al., [1] suggested examining the current state of open-source intelligence (OSINT), revealing the inadequacies of current techniques in real-world scenarios. This study emphasizes integrating OSINT into diverse domains such as cyber defenses, social networks, and digital forensics. The objective is to enhance capabilities in profiling culprits, investigating cybercrimes, countering terrorism, and addressing cyber incidents. The paper delineates fundamental OSINT search techniques and introduces advanced OSINT tools, highlighting the importance of selecting tools judiciously based on available data and objectives. Combining multiple tools is advocated for achieving more accurate results. The discussion extends to open-source data, social networks, various cybercrime typologies, and OSINT techniques augmented with Natural Language Processing (NLP), Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL). This integration is positioned as beneficial for investigators aiming to augment OSINT research and applications. Traditional Indicators of Compromise (IOCs) extracted from blacklists often lack contextual information about criminal groups. OSINT addresses this limitation by incorporating psychological and behavioral features.

The paper concludes that OSINT facilitates cybersecurity challenges across various domains, including phishing detection, threat intelligence, hate speech detection, fake news detection, human trafficking, and criminal profiling. Additionally, OSINT aids in monitoring Advanced Persistent Threat (APT) groups, analyzing fake images and videos, tracking malicious activities, and tracing violent acts. The study suggests leveraging automatic updating features, attack patterns, and IOCs for phishing detection to enhance model robustness and efficiency. However, several challenges persist, including extracting indicators of compromise and their relationships from unstructured threat intelligence reports, forming criminal consortia for tracking, developing comprehensive frameworks for OSINT tools and techniques, automating information gathering and intelligence extraction from open-source data using AI, establishing real-time monitoring of APT groups through OSINT and DL techniques, and creating multi-platform, multi-lingual benchmark datasets for cybercrime detection based on social networks

using OSINT tools and techniques. Addressing these challenges is essential for advancing the effectiveness and scope of OSINT in cybersecurity.

Carley et al., [2] highlight that social cybersecurity is an emerging scientific and engineering discipline, indicating the need for additional research and enhanced coordination within the field. Although numerous professionals contribute to this space, there is a recognized necessity for increased research efforts and improved collaboration. The evolution of work in social cybersecurity initially began as interdisciplinary and is progressing toward a transdisciplinary nature. It is important to exercise caution, particularly for those new to this area, as it may seem that the knowledge base is limited, and only a handful of individuals are actively engaged. This perception can be attributed to various factors, such as the dispersion of research across numerous venues without a dominant conference or journal. Social cybersecurity research tends to be on the fringes of existing disciplines. A significant challenge is that many researchers in this field are unaware of others beyond their immediate group or even within their university. There is a recognized need for greater outreach and improved collaboration mechanisms across different research groups, a trend gradually taking shape. The collaboration network illustrates the growth of a central core and the establishment of new links that were previously absent. This expansion can be largely attributed to support from initiatives such as the Department of Defense Minerva program and the Knight Foundation, which have played pivotal roles in fostering research in social cybersecurity and encouraging collaborative efforts.

Aboelfotoh and Hikal [3] address the pervasive integration of technology in both individual and enterprise settings. Given the substantial proliferation of technologies and electronic communications, they have become crucial pillars for the operational framework of enterprises, irrespective of size. These technologies also serve as primary sources of education and entertainment for individuals. Consequently, this heightened technological dependence has prompted a critical examination of the associated risks, necessitating experts and decision-makers to evaluate the potential impact on economic indices, market reputation, and overall safety for individuals and enterprises. In response to these concerns, there is a recognized need to reevaluate information security strategies, leading to the development of novel methodologies for measuring and assessing the protection of information and data within enterprises, as well as the privacy of individuals. This paper comprehensively reviews recent cybersecurity measuring and assessment methodologies and tools, aligning with industry best practices for evaluating network security and safeguarding modern enterprise data networks. The analysis is rooted in thoroughly examining methods for measuring and assessing information security at both the physical and technical levels. This includes an in-depth exploration of penetration testing and identifying weaknesses in cybersecurity systems and policies employed by contemporary enterprises. The paper thoroughly explores these tools' strengths, weaknesses, and licensing conditions. Furthermore, the paper delves into discussing and analyzing major security requirements relevant to modern enterprises. This aims to uncover vulnerabilities in existing systems and elucidate the potential impact of these vulnerabilities on the overall security posture. The technical depth of the examination extends to exploring the intricacies of contemporary cybersecurity measures, ensuring a nuanced understanding of the challenges and opportunities inherent in safeguarding enterprise data networks in the current technological landscape.

Markowsky and Markowsky [4] allude to the enduring wisdom encapsulated in the adage "a picture is worth a thousand words," a maxim that holds particular relevance in cybersecurity. In this realm, professionals grapple with the formidable challenge of processing substantial volumes of data within stringent time constraints. The significance of this adage extends to cybersecurity educators who must elucidate the intricacies of cybersecurity events, especially to audiences lacking a substantive background in the field. Fortunately, the evolution of visualization tools has yielded many sophisticated options, promising further advancements. This paper examines existing visualization tools, shedding light on commendable work that merits heightened recognition among cybersecurity educators. The seminal year 1983 witnessed Edward Tufte's groundbreaking contribution to information display with his seminal work, The Visual Display of Quantitative Information, which underwent multiple printings before a second edition materialized. Tufte's work catalyzed widespread interest in graphic design and the visual representation of information, paving the way for subsequent publications in the field, including notable works by William Cleveland. Despite the remarkable strides made in computing technology over recent decades, the cognitive capacity of humans has remained relatively constant. Thus, adherence to well-established design principles emerges as paramount when crafting visualizations for optimal comprehension by individuals.

Ferrag et al., [5] highlight the contemporary landscape where a substantial portion of critical global operations, spanning various sectors, relies on Industrial Control Systems (ICS). An archetypal ICS comprises an extensive array of computerized devices, control systems, and network appliances strategically deployed to efficiently manage industrial processes across expansive geographical areas. These systems are the linchpin for sensitive and crucial national infrastructures, including water treatment, energy production, and transportation. The repercussions of a successful attack on ICS are profound, potentially leading to the shutdown of critical infrastructures with far-reaching impacts, encompassing production halts and implications for the safety of individuals, the environment, and assets. Simultaneously, operating a process during an attack or compromise poses safety risks, potentially of catastrophic proportions. This work-in-progress focuses on an adaptive approach capable of dynamically adjusting the defensive posture while ensuring operational capacity (or appropriately degrading it) and maintaining safety. The

proposed approach involves the transformation of policies from mere enforcers of predefined security requirements to adaptive entities capable of evolving in response to unfolding attacks. The paper employs a case study that addresses reconnaissance attacks and leverages moving target defense to implement adaptive security policies.

Pratama and Wiradarma [6] emphasize the critical importance of timely information in ensuring robust cybersecurity for IT infrastructure. In the ever-evolving cybersecurity landscape, gathering the most recent and pertinent information is traditionally manual, labor-intensive, and exhaustive. While there is a push towards automated and user-friendly approaches to streamline this process, their effectiveness is contingent upon a nuanced understanding of information relevance to distinguish essential data from non-essential. To address this challenge, the paper conducts a comprehensive literature review and proposes a pioneering categorization of cybersecurity tools. This categorization is based on distinct tool types, each accompanied by precise definitions and core features. Subsequently, the paper delves into the specific information employed within each categorized tool and elucidates the criteria used to determine its relevance. This three-tiered approach lays the groundwork for a more systematic and informed utilization of cybersecurity tools. Building upon these insights, the paper describes the design of a security dashboard. This dashboard is a practical tool for computer emergency response team (CERT) staff, guiding them in identifying threats within open-source intelligence sources. The dashboard's design is strategically informed by the derived criteria for information relevance, ensuring that it aids CERT staff in navigating through the intricacies of real-time threats while mitigating the challenges associated with information overload. In essence, the paper not only contributes to a refined understanding of cybersecurity tool categorization and information relevance but also offers a practical solution in the form of a well-designed security dashboard to enhance the operational efficiency of cybersecurity professionals.

Kaushik et al., [7] introduce a comprehensive cyber security dataset for IoT and IIoT applications, named Edge-IIoTset, designed for application in machine learning-based intrusion detection systems operating in two modes: centralized and federated learning. The dataset is meticulously generated using a purpose-built IoT/IIoT testbed, featuring a diverse set of representative devices, sensors, protocols, and configurations spanning cloud and edge environments. The IoT data includes over ten types of devices: low-cost digital sensors for temperature and humidity sensing, ultrasonic sensors, water level detection sensors, pH sensor meters, soil moisture sensors, heart rate sensors, and flame sensors. Additionally, the authors identify and analyze fourteen attacks associated with IoT and IoT connectivity protocols, categorized into five threats: DoS/DDoS attacks, Information gathering, Man-in-the-middle attacks, Injection attacks, and Malware attacks. The feature extraction process incorporates data from various sources, including alerts, system resources, logs, and network traffic, resulting in the proposal of 61 new features with high correlations from 1176 identified features. After processing and analyzing this cyber security dataset, the paper conducts a primary exploratory data analysis. It evaluates the performance of machine learning approaches, encompassing both traditional machine learning and deep learning methods. The evaluation is conducted in both centralized and federated learning modes, providing valuable insights into the effectiveness of these approaches in addressing cyber security challenges in the IoT and IIoT domains.

Ferrag et al., [8] highlight the escalating trend of mobility facilitated by technological applications, specifically focusing on developing websites for information exchange and management. However, this increased technological reliance introduces inherent challenges, particularly regarding information disclosure, necessitating a meticulous evaluation of security and protection measures. Recognizing the imperative for robust website security, the authors advocate for applying penetration testing methods to systematically assess and identify vulnerabilities within the system. In this study, the authors embrace the Open Source Intelligence concept and employ Maltego as a pivotal tool for conducting security testing. They align their methodology with the OWASP version 4 framework, utilizing it as a standardized guide to ensure a comprehensive and structured approach to the security testing process. The specific focus of their investigation is directed towards the X Company's website, emphasizing conducting security testing to gather crucial information. The testing and subsequent analysis, conducted by the OWASP version 4 framework and specifically utilizing its Testing for Information Gathering module, provide insightful revelations about the vulnerabilities in the web application system employed by X Company. These vulnerabilities include exposure to information related to the web server version, susceptibility in GET and POST requests, discernible patterns in URL structuring, nuances in the website framework, vulnerabilities in the website builder component, and a comprehensive understanding of the overall architecture of the website. The study identifies potential weaknesses in the X Company's website by adopting a meticulous and systematic approach. It contributes to the broader discourse on website security methodologies, emphasizing the importance of standardized frameworks and tools in information security testing.

Swartz [9] emphasized that organizations worldwide proactively form teams of ethical hackers. These teams are tasked with collecting threat data to fortify their existing systems against ongoing cyber threats and cultivate a resilient cybersecurity workforce. Among the myriad tools available in the contemporary era, NMAP is a standout information-gathering program. This tool's efficacy is further underscored as the researcher employs NBTSCAN to instigate host scan attacks. The research undertaking involves a comprehensive data-gathering approach, encompassing live and inactive forensics data. A notable step in this process is the analysis of DHCP requests, a crucial element in tracing the origin of the attacking laptop. To paint a comprehensive picture of the cybersecurity landscape, the researchers adopt multiple network scanning tools, aggregating

diverse reports in various formats. A noteworthy aspect of the methodology employed is the automation of information source access. This automation streamlines the information-gathering process, enhancing efficiency and effectiveness. Ultimately, the various techniques employed for information gathering are underscored as instrumental in acquiring essential and pertinent information, contributing significantly to the overall cybersecurity efforts.

Friedman and Hoffman [10] assert the timeless wisdom encapsulated in the adage "Knowledge is power," finding its resonance in today's information age. They underscore that knowledge, in contemporary terms, stems from unfettered access to information. The capacity to extract valuable insights from vast datasets has emerged as a matter of paramount significance. Researchers have coined the term Big Data Analytics (BDA) to encapsulate the processes of processing, storing, and gathering extensive data for subsequent analysis. The exponential production of data has become a critical issue, with the proliferation of the Internet, Internet of Things (IoT), and other technological advancements being primary contributors to this sustained growth. The generated data serves as a mirror reflecting the environment from which it originates. Consequently, leveraging the data obtained from systems provides a means to decipher those systems' internal workings, a pivotal aspect in cybersecurity, where the primary objective is safeguarding assets. Furthermore, the escalating value of data has elevated big data to a high-value target. The paper delves into recent research in cybersecurity concerning big data, shedding light on the protective measures for big data and its role as a tool in cybersecurity. The authors present their findings in tables, summarizing recent works and outlining trends, open research challenges, and existing problems. Through this comprehensive exploration, readers gain a more profound understanding of cybersecurity in the era of big data, along with insights into research trends and the prevailing challenges within this dynamic and actively researched domain.

Ghorbanzadeh et al., [11] highlight the global landscape where organizations employ teams to gather threat data to fortify their defences against incoming cyber-attacks and maintain a robust cybersecurity posture. These teams focus on internal data collection and share information, recognizing the need for external insights to form a comprehensive view of the ever-evolving threat landscape. Cyber threat information is derived from diverse sources, including sharing communities and open-source and commercial channels, spanning various levels and timeframes. Immediately actionable information typically involves low-level indicators of compromise, such as known malware hash values or command-and-control IP addresses, enabling automated responses by systems. In contrast, threat intelligence encompasses more intricate cyber threat details acquired or inferred through comprehensive analysis. This sophisticated information includes insights into the evolution of malware families used over time, the network of threat actors involved in an attack, and other valuable details crucial for understanding, predicting, and responding to cyber threats. Importantly, applying threat intelligence often necessitates human intervention, involving collaboration with multiple intelligence sources, data combination and enrichment, determination of relevance based on technical constructs and organizational input, and integration into organizational workflows and technological products. The paper encountered challenges in this realm. It summarized community requirements and expectations for a comprehensive Threat Intelligence Management Platform, addressing the intricate and multifaceted nature of managing and leveraging threat intelligence in contemporary cybersecurity landscapes.

Lim et al., [12] delves into examining machine learning (ML) tools within artificial intelligence (AI), specifically optimizing their effectiveness when applied to address cybersecurity issues. The principal objective of the report is to provide nuanced guidance tailored for managers and decision-makers who are deliberating the implementation of ML for cybersecurity purposes. In the context of this report, the definitions of ML and AI have been intentionally narrowed to serve as precision parameters for ensuing discussions. As articulated within this framework, machine learning is construed as a suite of statistical tools meticulously engineered to scrutinize data sets. The overarching aim is to discern intricate relationships and patterns latent within the data. The aspirational outcome of this analytical process is constructing a robust and practically applicable model encapsulating the essence of the object or phenomenon under examination. In artificial intelligence, the document defines AI as a sophisticated software agent characterized by its capacity to execute actions contingent upon its environmental inputs. It is imperative to underscore that, according to this report's stipulations, AI's ambition is expressly not aligned with realizing the speculative notion of creating a sentient robot, as often portrayed in science fiction narratives.

Cremers [13] highlight the ongoing digitization of our world, which, while offering numerous benefits, also exposes us to an escalating frequency of cyber-attacks orchestrated by cyber criminals. Addressing this surge in cyber threats necessitates a substantial increase in cybersecurity professionals. Despite concerted efforts by academia and industry to bolster the ranks of cybersecurity experts, a significant shortage persists. Compounding this issue is the observation that the tools and techniques employed for the professional development of cybersecurity experts are proving ineffective. Consequently, the gap between the demand for and availability of cybersecurity professionals continues to widen. A pivotal component in cybersecurity professional development is hands-on cybersecurity exercises. This position paper critically examines the inefficiencies inherent in executing such exercises and proposes strategies to mitigate and ultimately eliminate these inefficiencies. The analysis presented herein delves into the challenges associated with hands-on cybersecurity exercises and explores viable avenues for improvement to enhance the overall efficacy of cybersecurity professional development initiatives.

Narayanan et al., [14] introduced a comprehensive guide tailored for universities and organizations aiming to conduct cybersecurity exercises. The outlined methodology is derived from synthesizing academic papers produced after various cybersecurity exercises. The guide systematically details seven essential steps to organize such exercises. Each step is meticulously explained, and the authors provide alternative options for implementation. The significant contribution of this paper is its provision of a versatile method for structuring a cybersecurity exercise. This method is designed to be adaptable, allowing organizers to tailor it to their specific needs and objectives. Unlike previous works that predominantly focus on documenting frameworks for cybersecurity education [3] or provide analyses, overviews, opinions, and questions about the generalization of cybersecurity exercises [1], George et al.'s paper offers a practical, hands-on approach. It highlights the steps involved and considers the diverse ways they can be implemented, providing a valuable resource for those involved in organizing and executing cybersecurity exercises.

Berger and Jones [15] address the impact of the Fourth Industrial Revolution on conventional practices in the digital space. Cybersecurity strategies are increasingly recognized as central and crucial components of digital transformations as this revolution disrupts established norms. In this context, cybersecurity pertains to intelligently designed processes and networks to safeguard digital assets from unauthorized access. The authors contribute insights into how businesses can align their operations within cybersecurity driven by Industry 4.0 technologies, ultimately fostering sustainability. The initial step involves gathering perceptions from network and security solution organizations. Subsequently, the collected cybersecurity initiatives are employed to explore a system dynamics model. The results offer valuable insights for strategic and tactical decision support in business, aiding in mitigating potential cybersecurity breaches and threats.

In the rapidly evolving landscape of academic research, particularly in recent years, it is evident that each work contributes its unique strengths and faces specific challenges. The diversity in approaches and methodologies across these works underscores the complexity and multifaceted nature of the subjects under investigation. This paper takes a critical stance, addressing the challenges encountered by existing works, aiming to contribute to a nuanced understanding of the broader research landscape. The proliferation of research efforts across various domains has led to a wealth of knowledge, with each work presenting its own set of advantages and limitations. This diversity is a testament to the richness of ideas and perspectives within the academic community. However, challenges are inevitable, and recognizing and addressing these challenges is vital for advancing knowledge and refining research methodologies. The primary focus of this paper is to elucidate the challenges existing works face. By undertaking a comprehensive examination, the authors aim to highlight areas where improvements and innovations are needed. Understanding the limitations of current research provides a foundation for future scholars to build upon, fostering a collaborative and iterative process of knowledge development. The paper provides a comprehensive summary of existing works in Table 1 to facilitate a structured exploration of the challenges. This tabulated overview serves as a valuable reference point for readers, offering a snapshot of the diverse research landscape. Each entry in the table encapsulates the essence of a particular work, summarizing its key contributions and, equally importantly, outlining the challenges encountered during its execution. The challenges outlined in the paper may encompass various dimensions, including methodological constraints, data limitations, or theoretical gaps.

By systematically analyzing these challenges, the authors contribute to the ongoing discourse within their specific domain and provide insights that may have broader implications for research practices across disciplines. This paper serves as a critical reflection on the current state of academic research by addressing the challenges inherent in existing works. It invites readers to consider the nuanced interplay between the strengths and limitations of research endeavors, emphasizing the importance of an iterative and collaborative approach to knowledge creation. Through this exploration, the authors aim to inspire future researchers to navigate the complex terrain of academic inquiry with a heightened awareness of the challenges and opportunities that shape the research landscape.

Table 1: Summary of Literature reviews

Author	Methodology	Technical Gap
Carley et al., [2]	Dynamic network analysis, Simulating the spread of information or behaviors within complex systems in cybersecurity	• User Data Collection and Privacy • Dynamic Network Analysis Challenges • Complex Systems Information Spread Challenges
Yadav et al. [1]	OSINT research techniques in cybersecurity	• Information Overload • Source Reliability • Attribution Difficulty • Privacy Concerns • Technological Changes • Legal and Ethical Boundaries

Ferrag et al., [5]	Industrial control systems (ICS) in cybersecurity	• Cybersecurity Vulnerabilities • Interconnected System Risks • Legacy System Compatibility • Lack of Standardization
Kaushik et al., [7]	Big Data Analytics, Internet of things in cybersecurity	• Data Privacy Concerns • Ensuring Data Accuracy • Managing Large Volumes of Data • Extracting Meaningful Insights • Data Security and Protection
Ferrag et al. [8]	Machine learning (ML) tools for Artificial Intelligence (AI) in cybersecurity	• Adversarial Attacks • Lack of Explainability • Data Privacy Concerns • Resource Intensiveness • Integration Complexity • Evolving Threat Landscape • Talent Shortage in AI Security • Ethical and Regulatory Challenges

3. Methodology

A strong approach is essential while collecting information in cybersecurity to safeguard digital assets and uphold security. The following is a cybersecurity information gathering tools methodology (Figure 1):

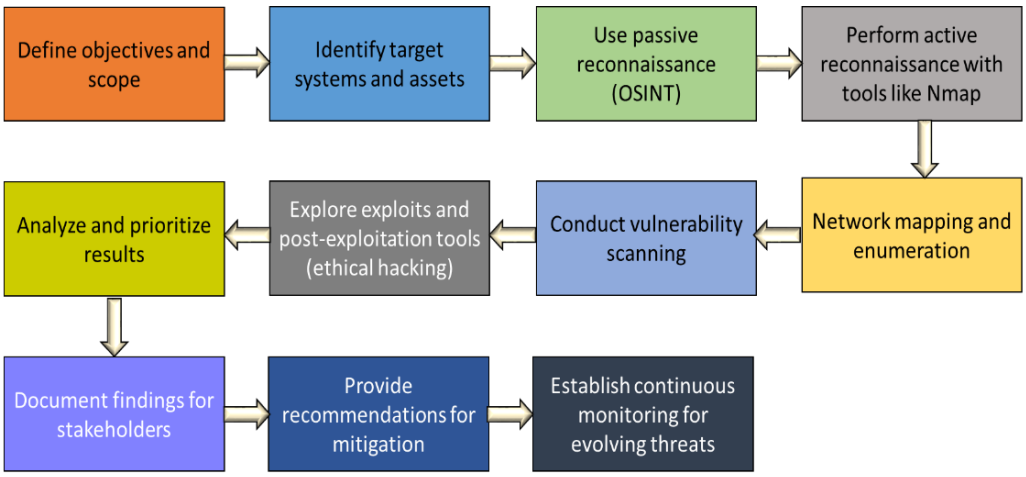

Figure 1: Functional Block Diagram of cybersecurity information gathering

3.1. Define Objectives and Scope

A fundamental step marks the inception of any cybersecurity information-gathering endeavor — the meticulous definition of objectives and delineation of the assessment's scope [29]. This initial phase serves as the cornerstone for the entire process, setting the tone for subsequent actions and laying the groundwork for a comprehensive and effective security evaluation. At the heart of this foundational step is clearly articulating the goals that steer the information-gathering initiative. These objectives form the guiding principles, directing the efforts towards specific outcomes. Whether the primary focus is identifying vulnerabilities, scrutinizing network architecture, or conducting an overarching evaluation of the security posture, formulating these goals is paramount [30]. The precision and clarity with which the objectives are defined directly influence the success and relevance of the subsequent stages in the cybersecurity assessment [31].

Furthermore, establishing the scope of the assessment emerges as a critical aspect of this initial step. The scope acts as a virtual perimeter, demarcating the boundaries within which the evaluation will unfold. This delineation is essential to avoid ambiguity and ensure a focused and targeted approach. Without a clearly defined scope, the assessment could become unwieldy, potentially leading to inefficiencies and a lack of specificity in the findings [32]. Defining the scope involves carefully considering the systems, networks, and assets that will fall under the purview of the assessment. This decision is guided by the

overarching objectives, ensuring that the chosen scope aligns with the goals set for the information-gathering initiative [33]. Within these boundaries, the cybersecurity professionals will direct their efforts, honing in on specific elements deemed crucial to the security evaluation. Moreover, a well-defined scope enables the cybersecurity team to allocate resources judiciously. By clearly outlining what is within the assessment's scope and what lies outside it, the team can optimize efforts and concentrate on areas most pertinent to the identified goals [34]. This focused approach enhances the efficiency of the information-gathering process, allowing for a more in-depth analysis of the targeted systems and networks [35].

The significance of defining objectives and scope in the cybersecurity information-gathering process cannot be overstated. It is the pivotal point at which the overarching goals are crystallized, providing a roadmap for subsequent actions [36]. The clarity achieved in this initial step becomes the bedrock for effective decision-making, resource allocation, and, ultimately, the success of the entire cybersecurity assessment. As the process unfolds, this clarity ensures that every action is purposeful and contributes meaningfully to attaining the predefined objectives, resulting in a robust and well-informed security posture for the organization [37].

3.2. Identify Target Systems and Assets

The objectives and scope of a cybersecurity information-gathering initiative are clearly defined; the subsequent crucial step is identifying target systems and assets. This phase represents operationalizing the strategic goals, transforming overarching objectives into tangible, actionable tasks. Pinpointing specific systems within the established scope is pivotal for conducting a thorough and effective security assessment [38]. The first imperative task in this phase is to create a comprehensive list of target systems. This list encompasses diverse critical components within the designated scope, from servers and databases to network devices and overarching critical infrastructure. Each element on this list plays a unique role in the organization's digital ecosystem, making it essential to cast a wide net to ensure a holistic assessment of the security landscape. Servers warrant meticulous attention as the backbone of information storage and retrieval [39]. Identifying server vulnerabilities is crucial, given their central role in housing sensitive data and managing network operations. Databases, where a wealth of organizational information is stored, also emerge as critical targets for examination. The security of databases is paramount to prevent unauthorized access and safeguard the integrity of stored data [40].

The network devices, including routers, switches, and firewalls, form the intricate web through which digital communications flow. Evaluating the security of these devices is essential for fortifying the organization's network against potential threats and vulnerabilities [41]. Additionally, critical infrastructure components, such as power systems, HVAC (heating, ventilation, and air conditioning), and other essential utilities, need careful consideration to ensure the overall resilience of the organizational ecosystem. Prioritization becomes pivotal in this phase, guiding the cybersecurity team to allocate resources judiciously and strategically. Given the diverse nature of the target systems, prioritization enables a more systematic and efficient information-gathering process [42]. By categorizing systems based on their criticality and potential impact on the organization, the team can tailor their efforts to focus on high-priority areas [43]. This prioritization strategy ensures that the most critical and vulnerable systems are addressed promptly, minimizing the risk of overlooking significant security threats. It also allows for a phased approach, enabling the cybersecurity team to manage the information-gathering process in a structured manner. In essence, prioritization aligns the information-gathering efforts with the overarching goals and objectives, making the process efficient and highly strategic [44].

Identifying target systems and assets is a pivotal phase in cybersecurity information gathering. It transforms abstract objectives and scope into concrete tasks, guiding the cybersecurity team to specific components within the organization's digital infrastructure [45]. The comprehensive list created during this phase serves as a roadmap for subsequent actions, ensuring the security assessment is thorough, systematic, and strategically aligned with the organization's security goals. Through careful prioritization, the cybersecurity team can navigate the complexity of the digital landscape, addressing high-priority areas first and fortifying the organization against potential cyber threats [46].

3.3. Use Passive Reconnaissance

Passive surveillance, distinguished by its non-intrusive nature, constitutes a pivotal phase in the cybersecurity information-gathering. This strategic step systematically gathers information without direct interaction with the target systems, emphasizing the importance of discretion and stealth. Using Open-source Intelligence (OSINT) tools emerges as a cornerstone, enabling cybersecurity professionals to access and collect publicly available information [47]. This phase establishes a nuanced and comprehensive understanding of the target environment. Open-source intelligence tools are the linchpin of passive surveillance, providing cybersecurity professionals with a suite of instruments to navigate the vast landscape of publicly accessible information [48]. The inherent openness of these sources allows analysts to glean insights without triggering alerts or raising suspicions, aligning with the clandestine nature of the information-gathering process. OSINT tools aggregate data from diverse sources, including online forums, websites, and public records, offering a panoramic view of the target's digital footprint [49].

Analysts adept in passive reconnaissance might delve into social media platforms during this phase, scouring profiles, posts, and connections to extract valuable nuggets of information. The seemingly innocuous details shared by individuals and organizations on social media can contribute to constructing a comprehensive profile. Public databases, another bastion of information, are meticulously combed for domain registration information, historical data, and affiliations. By harnessing these non-intrusive sources, analysts compile a mosaic of data points that lay the groundwork for subsequent stages in the cybersecurity assessment. The non-intrusive nature of passive surveillance is advantageous as it avoids direct contact with the target systems. This discretion is vital, especially when the assessment is conducted for defensive or investigative purposes, as it minimizes the risk of alerting the target to ongoing reconnaissance activities. Cybersecurity professionals can gain valuable insights by relying on publicly available data while adhering to ethical and legal standards.

Furthermore, a passive survey serves as the survey's initial building block, setting the stage for a deeper dive into the intricacies of the target environment. The information gathered in this phase provides a baseline understanding of the target's online presence, affiliations, and potential vulnerabilities. It offers the cybersecurity team a strategic advantage by informing subsequent actions in the information-gathering process, guiding the allocation of resources, and shaping the overall approach to the security assessment. Passive reconnaissance is a discreet yet powerful phase in the cybersecurity information-gathering process. By leveraging OSINT tools to sift through publicly available information, analysts construct a preliminary profile of the target without triggering alerts. The insights gleaned during this phase lay the groundwork for a more profound understanding of the target environment, guiding subsequent actions in the security assessment. In navigating the complexities of cyberspace, passive reconnaissance emerges as a crucial precursor to more intrusive phases, contributing to a holistic and strategic approach to cybersecurity.

3.4. Perform Active Reconnaissance

The active survey is a pivotal phase in cybersecurity information gathering, characterized by its engaged and probing nature. In contrast to passive surveillance, which focuses on discreetly collecting publicly available information, active surveillance involves direct interaction with the target systems. This hands-on approach is instrumental in acquiring more detailed and specific information, allowing cybersecurity professionals to delve deeper into the intricacies of the target environment. Tools like Nmap take center stage in this phase, conducting active scanning and employing enumeration techniques to extract critical insights. The cornerstone of active surveillance is deploying sophisticated tools such as Nmap, a powerful network scanning utility. Nmap plays a crucial role in information gathering by actively probing the target network and identifying live hosts, open ports, and services. Live hosts signify current operational systems, providing a foundation for subsequent analysis. Open ports and services, on the other hand, reveal entry points and potential vulnerabilities in the target's network architecture.

One of the primary functionalities of Nmap is its ability to conduct comprehensive port scans. By systematically probing each port on a target system, Nmap uncovers open ports, indicating potential avenues for exploitation. Identifying these open ports is instrumental in understanding the network's topology and potential weak points that malicious actors could exploit. In addition to port scanning, active surveillance involves applying enumeration techniques to gather further insights into the identified systems. Enumeration encompasses the systematic extraction of information about the target, such as version numbers and configurations of operating systems and services. This granular level of detail is crucial for cybersecurity professionals to understand the specific technological landscape of the target environment. Enumeration techniques extend beyond simple identification, providing a more in-depth understanding of the target systems. For instance, services running on identified open ports may reveal specific software versions, allowing analysts to assess the presence of known vulnerabilities associated with those versions. This information is invaluable in shaping subsequent stages of the security assessment, guiding the focus towards areas with a higher potential for exploitation.

Active surveillance, emphasizing direct interaction and tool-assisted probing, provides a dynamic and real-time assessment of the target environment. This approach allows cybersecurity professionals to uncover potential vulnerabilities that might not be evident through passive means. However, it is essential to note that active reconnaissance carries a higher detection risk than passive methods, potentially alerting the target to the ongoing assessment. Active surveillance represents a crucial phase in cybersecurity information-gathering, bringing a dynamic and hands-on dimension to the assessment. Tools like Nmap play a central role in actively scanning and probing the target network and identifying live hosts, open ports, and services. Enumeration techniques further enhance the depth of understanding by extracting specific details about the target systems. While active surveillance introduces a higher level of engagement, it provides a nuanced and real-time perspective, allowing cybersecurity professionals to make informed decisions and prioritize areas of focus for subsequent phases in the security assessment.

3.5. Network Mapping and Enumeration

Network mapping and enumeration are foundational to comprehending the target's network architecture within cybersecurity

information-gathering. These phases play a crucial role in developing a holistic understanding of the target's digital landscape, facilitating the visualization of network structures, relationships between systems, and potential avenues for exploitation. Cybersecurity professionals can glean critical insights, identify vulnerabilities, and extract detailed information through systematic techniques, contributing to a thorough security assessment. The initiation of this phase mandates the creation of a detailed network map. This graphical representation visually delineates the target's network architecture, illustrating the interconnections among systems, devices, and infrastructure components. This visual aid assists cybersecurity professionals in grasping the network layout, pinpointing entry and exit points, and recognizing potential chokepoints or bottlenecks. Visualizing the network's structure serves as a strategic guide for subsequent actions in the security assessment.

As a strategic tool, the network map enables professionals to comprehend the relationships between systems and discern patterns, dependencies, and potential vulnerabilities. This holistic perspective is instrumental in strategizing the assessment, allocating resources judiciously, and prioritizing areas for in-depth scrutiny. A comprehensive network map establishes the foundation for a targeted and effective cybersecurity evaluation. Following the network mapping, the next imperative is enumeration, a process that involves extracting detailed information about the identified systems within the network. Unlike surface-level assessments, enumeration delves into specifics such as user accounts, shared resources, and network configurations. Enumeration techniques are crafted to unveil the intricate layers of the target environment, furnishing cybersecurity professionals with a nuanced understanding of the digital ecosystem under assessment.

A crucial facet of enumeration is the extraction of user account information. This encompasses identifying user names, privileges, and roles within the network. A profound understanding of the user landscape is pivotal, as compromised user accounts often serve as gateways for malicious actors. Additionally, enumeration reveals shared resources and network assets, shedding light on critical infrastructure components and potential points of vulnerability. The insights garnered through enumeration significantly augment the depth of the security assessment. Cybersecurity professionals can unearth potential weak points, evaluate the overall security posture, and prioritize remediation efforts based on the severity of identified vulnerabilities. The detailed information obtained during enumeration guides subsequent actions, providing a structured approach for penetration testing, vulnerability mitigation, and overall network fortification. Network mapping and enumeration are pivotal steps in cybersecurity information gathering. Creating a detailed network map facilitates the visualization of the target's architecture, aiding in identifying relationships between systems and potential pathways for exploitation. Enumeration, taking the assessment to a granular level, extracts detailed information about user accounts, shares, and network resources. These systematic steps collectively contribute to a comprehensive understanding of the target environment, empowering cybersecurity professionals to make informed decisions and enhance the overall security posture.

3.6. Vulnerability Scanning

Vulnerability scanning tools play a crucial role in the cybersecurity assessment, utilizing advanced capabilities to identify known vulnerabilities within target systems. Prominent among these tools are Nexpose and Nessus, which conduct systematic scans across the network infrastructure to pinpoint potential weaknesses that malicious actors could exploit. This proactive approach provides cybersecurity professionals with a quantitative assessment of the security posture, enabling them to prioritize remediation efforts based on the severity of identified vulnerabilities. Nexpose and Nessus exemplify robust vulnerability scanning tools, leveraging comprehensive databases of known vulnerabilities and employing sophisticated scanning techniques. These tools meticulously examine each system, application, and device within the designated scope, ensuring a thorough assessment of the entire network. The systematic nature of these scans goes beyond surface-level evaluations, delving deep into the intricacies of each component to identify potential security gaps.

One of the distinctive advantages of vulnerability scanning tools lies in their ability to generate quantitative metrics that reflect the severity and potential impact of identified vulnerabilities. Risk scores or severity levels are assigned to each vulnerability, indicating the criticality of the discovered issues. This quantitative data facilitates informed decision-making, allowing cybersecurity professionals to prioritize remediation efforts based on the criticality of the vulnerabilities. The comprehensive reports generated by vulnerability scanning tools serve as invaluable resources for cybersecurity professionals and decision-makers. These reports offer a detailed overview of the security landscape, presenting identified weaknesses and associated risk scores. By providing this granular information, vulnerability scanning tools empower organizations to make strategic decisions regarding allocating resources for remediation efforts.

The strategic prioritization facilitated by vulnerability scanning tools ensures that cybersecurity teams focus on addressing high-severity vulnerabilities first. This targeted approach enhances the efficiency of remediation efforts, addressing the most critical issues that pose significant risks to organizational assets and data. By systematically addressing vulnerabilities in order of severity, organizations can fortify their defences and reduce the likelihood of successful cyberattacks. Regularly utilizing vulnerability scanning tools contributes to continuously improving an organization's security posture. Organizations can establish a proactive cybersecurity stance by staying vigilant and promptly addressing identified vulnerabilities. This proactive

approach is essential in mitigating potential risks and enhancing resilience against evolving cyber threats in the dynamic landscape of digital security. Vulnerability scanning tools such as Nexpose and Nessus play a pivotal role in cybersecurity assessments. These tools provide a quantitative security posture assessment by systematically identifying known vulnerabilities. The generated reports enable strategic prioritization of remediation efforts, allowing organizations to strengthen their defenses and maintain a proactive cybersecurity stance in the face of evolving cyber threats.

3.7. Exploit and Post-Exploitation

In ethical hacking scenarios, penetration testing tools are pivotal in simulating cyberattacks and discerning potential vulnerabilities within a system or network. This proactive approach empowers cybersecurity professionals to assess the robustness of defences and identify weaknesses before malicious entities can exploit them. The penetration testing process typically involves three main categories of tools: exploitation tools, scrutinizing the system's resilience against diverse attack vectors, and post-exploitation tools, evaluating the aftermath of a successful attack by extracting additional information and scrutinizing potential persistence mechanisms. Exploitation tools constitute a crucial phase in penetration testing, aiming to evaluate the system's ability to withstand various attack vectors that real-world adversaries might deploy. These tools are adept at exploiting known vulnerabilities, revealing potential weaknesses susceptible to exploitation by malicious actors. By replicating the tactics, techniques, and procedures employed by actual attackers, ethical hackers gain insights into the efficacy of existing security measures and pinpoint areas necessitating improvement. Prominent examples of exploitation tools encompass Metasploit, Cobalt Strike, and BeEF, each offering a range of capabilities to simulate diverse cyberattacks.

Following the exploitation phase, post-exploitation tools come into play, concentrating on assessing the impact of a successful attack. Once a system has been compromised, these tools assist ethical hackers in delving deeper into the system, extracting additional information, and evaluating potential persistence mechanisms enabling unauthorized access to persist over time. Post-exploitation tools furnish valuable insights into the extent of the breach, potential data exposure, and the overall impact on the target system. Noteworthy examples of post-exploitation tools include PowerSploit, Empire, and Covenant, featuring functionalities like privilege escalation, lateral movement, and data exfiltration. Integrating these penetration testing tools is pivotal in comprehensively understanding a system's security posture. Ethical hackers can identify the vulnerabilities leading to the initial compromise and potential avenues for further exploitation and compromise. This holistic assessment allows organizations to proactively address security gaps, fortify defenses, and elevate their cybersecurity resilience.

Furthermore, ethical hacking scenarios frequently involve the collaboration of penetration testers with the organization's security teams to comprehend and implement effective remediation strategies. By leveraging penetration testing tools, organizations can stay ahead of potential adversaries, consistently improving their security posture and fostering a proactive cybersecurity culture. The penetration testing tools assume a central role in ethical hacking scenarios by simulating cyberattacks, identifying vulnerabilities, and evaluating the impact of successful breaches. Exploitation tools scrutinize system resilience against diverse attack vectors, while post-exploitation tools assess the aftermath by extracting additional information and evaluating potential persistence mechanisms. This systematic approach enables organizations to proactively enhance their security measures, address vulnerabilities, and cultivate a resilient cybersecurity environment in the face of evolving cyber threats.

3.8. Analyze Results

The analysis phase in cybersecurity represents a critical stage wherein the information collected from diverse tools undergoes meticulous scrutiny by cybersecurity analysts. This phase is paramount in converting raw data into actionable insights, empowering analysts to assess patterns, discern trends, and reveal potential security risks within the organization's digital ecosystem. The primary objectives of the analysis phase encompass prioritizing vulnerabilities based on severity and evaluating their potential impact on the organization's overall security posture. Success in this phase hinges on a sophisticated understanding of the security landscape and the ability to interpret complex datasets accurately. Cybersecurity analysts assume a central role in unraveling the information acquired from various sources, including vulnerability scans, network maps, threat intelligence feeds, and logs. These disparate datasets provide information about the organization's digital infrastructure, potential vulnerabilities, and ongoing security threats. The analysis phase serves as the linchpin, transforming this raw information into actionable intelligence that guides organizations in strengthening their defenses and proactively addressing security challenges.

Patterns and trends within the data undergo meticulous scrutiny during the analysis phase. Analysts leverage their expertise to discern recurring themes, identify unusual activities, and pinpoint anomalous patterns that may indicate potential security incidents. Detecting these patterns is instrumental in identifying sophisticated cyber threats that might go unnoticed. Through a nuanced understanding of the data, analysts uncover hidden connections and correlations, providing valuable context for decision-making. A key task during the analysis phase is the prioritization of vulnerabilities. Recognizing that not all

vulnerabilities pose an equal risk, prioritization ensures efficient resource allocation to address the most critical issues first. Severity assessments categorize vulnerabilities based on their potential impact and exploitability. This risk-based approach empowers organizations to concentrate efforts on mitigating vulnerabilities that pose the greatest threat to their cybersecurity posture.

The ability to interpret complex datasets is a hallmark skill of cybersecurity analysts during the analysis phase. Information gathered from various tools often arrives in diverse formats and structures, necessitating analysts to comprehensively understand cybersecurity frameworks, protocols, and attack vectors. This technical proficiency enables analysts to make sense of intricate data sets, drawing meaningful conclusions and actionable insights that inform subsequent actions. Moreover, the analysis phase is not a one-time event but an iterative process. Continuous analysis becomes essential to avoid potential risks as the threat landscape evolves and new vulnerabilities emerge. Regular assessments ensure that organizations maintain a proactive approach to cybersecurity, adapting their defenses to the dynamic nature of cyber threats. The analysis phase in cybersecurity is a pivotal stage where information collected from various tools undergoes meticulous scrutiny to assess patterns, discern trends, and reveal potential security risks. Cybersecurity analysts play a crucial role in transforming raw data into actionable intelligence, prioritizing vulnerabilities based on severity, and interpreting complex datasets. This phase is essential for organizations seeking to fortify their defenses, mitigate risks, and maintain a proactive stance against the evolving landscape of cyber threats.

3.9. Document Findings

Comprehensive documentation plays a pivotal role in the cybersecurity assessment as a foundational element for capturing and conveying all relevant information gathered throughout the assessment phases. This documentation encompasses critical details, including identified vulnerabilities, network maps, potential attack vectors, and other noteworthy findings. Creating clear and concise documentation is paramount, as is facilitating effective communication with stakeholders and providing them with actionable insights for remediation. The documentation process commences with the meticulous recording of identified vulnerabilities. This involves a detailed account of each vulnerability, specifying its nature, severity level, and potential impact on the organization's systems. Vulnerabilities may encompass a spectrum from software vulnerabilities and misconfigurations to potential weaknesses in network infrastructure. The documentation serves as a comprehensive inventory of security gaps within the organization, establishing the groundwork for a strategic and targeted remediation plan.

Network maps, another integral documentation component, visually represent the organization's digital landscape. These maps illustrate the interconnections between systems, devices, and infrastructure components. In the context of cybersecurity assessments, network maps assist stakeholders in visualizing potential pathways that malicious actors could exploit. A nuanced understanding of the organization's digital architecture is crucial for making informed decisions on security measures and allocating resources judiciously. The documentation further explores potential attack vectors, elucidating the methods and pathways adversaries might employ to exploit vulnerabilities. This section provides a narrative contextualizing the identified vulnerabilities within the broader scope of potential cyber threats. Organizations gain insights into adversaries' tactics by articulating possible attack vectors, empowering them to fortify defenses against specific threats.

Clarity and conciseness are paramount in documentation for effective communication with stakeholders. Cybersecurity professionals must convey complex technical information in a manner accessible to a diverse audience, including non-technical stakeholders such as executives and decision-makers. Concise documentation ensures stakeholders can swiftly grasp key insights, understand the severity of identified vulnerabilities, and make informed decisions regarding remediation strategies. Effective communication is a linchpin in the cybersecurity assessment process; documentation is the primary means to achieve this. Stakeholders, ranging from IT teams to executive leadership, rely on documentation to comprehend cybersecurity, the organization's potential risks, and the recommended actions for remediation. Clear documentation facilitates collaboration among different teams, aligning efforts toward enhancing the organization's security posture.

Moreover, documentation is valuable for post-assessment activities, including audits, compliance reporting, and future security planning. Well-documented assessments contribute to the organization's institutional knowledge, creating a historical record of cybersecurity efforts. This documentation becomes a reference point for tracking progress, assessing the effectiveness of remediation measures, and informing strategic decisions in subsequent cybersecurity initiatives. The comprehensive documentation is a fundamental aspect of the cybersecurity assessment process. It captures critical information on identified vulnerabilities, network maps, potential attack vectors, and other significant findings. Creating clear and concise documentation is essential for effective communication with stakeholders, providing them with actionable insights for remediation. Beyond immediate remediation efforts, well-documented assessments contribute to the organization's cybersecurity resilience, knowledge base, and strategic planning for future security endeavors.

3.10. Recommendations and Mitigation

The cybersecurity team assumes a crucial role in providing recommendations to mitigate identified vulnerabilities and fortify the organization's overall security posture. This phase represents a proactive response to the insights garnered during the analysis, with the overarching objective of delivering actionable strategies to guide remediation efforts. The recommendations are typically prioritized based on risk assessment and potential impact, ensuring a strategic and targeted approach to strengthening defenses against potential cyber threats. The recommendations phase is a pivotal component of the cybersecurity assessment lifecycle, serving as the bridge between identifying vulnerabilities and implementing effective remediation measures. The insights derived from the analysis phase lay the groundwork for crafting tailored recommendations that address the specific security challenges faced by the organization. These recommendations go beyond merely identifying vulnerabilities; they provide a roadmap for enhancing cybersecurity, aligning with the organization's unique risk landscape.

Prioritization is a key consideration in the recommendation phase. Not all vulnerabilities carry the same level of risk, and not all remediation measures have an equal impact on the overall security posture. Therefore, cybersecurity teams meticulously assess the identified vulnerabilities, assigning priority levels based on the severity of the risks they pose and the potential impact on the organization. This risk-based prioritization ensures that resources are allocated efficiently to address the most critical issues first, enhancing the organization's ability to thwart potential cyber threats effectively. The recommendations offer actionable insights that empower organizations to take decisive steps in bolstering their cybersecurity defenses. These insights are tailored to the organization's specific context, considering factors such as its industry, regulatory environment, and the criticality of its digital assets. Cybersecurity teams facilitate a seamless transition from assessment findings to proactive remediation efforts by providing clear and actionable recommendations.

Recommendations encompass a spectrum of cybersecurity measures, from patching identified vulnerabilities and strengthening access controls to implementing robust incident response plans and enhancing employee training on cybersecurity best practices. Each recommendation is crafted to address not only the immediate vulnerabilities but also contribute to the organization's long-term resilience against evolving cyber threats. Moreover, the recommendations phase extends beyond technical aspects to encompass broader aspects of cybersecurity governance and culture. Cybersecurity teams may advocate for establishing robust cybersecurity policies, regular training programs for employees, and integrating cybersecurity considerations into the organization's overall risk management strategy. These holistic recommendations aim to create a comprehensive and sustainable cybersecurity framework beyond immediate remediation efforts. The recommendations phase in cybersecurity assessments is a critical juncture where insights derived from the analysis phase are transformed into actionable strategies for enhancing an organization's security posture. These recommendations are prioritized based on risk assessment and potential impact, ensuring a focused and strategic approach to remediation efforts. By providing clear and actionable insights, cybersecurity teams empower organizations to fortify their defenses against potential threats, contributing to a resilient cybersecurity stance in the face of evolving cyber risks.

3.11. Continuous Monitoring

Establishing processes for continuous monitoring is paramount to maintaining an adaptive and robust cybersecurity posture in the face of evolving threats. The dynamic nature of threat landscapes and the emergence of new vulnerabilities necessitate a proactive and ongoing approach to staying informed about changes in the target environment. Cybersecurity is a field where change is constant, with threat actors consistently devising new tactics and exploiting novel vulnerabilities. Continuous monitoring is a proactive strategy to keep pace with these changes, providing organizations real-time insights into the evolving threat landscape. By routinely updating information and reassessing the security posture, organizations can effectively adapt their defenses to address emerging threats promptly.

Continuous monitoring is not a one-time effort but an ongoing process that involves the regular collection, analysis, and interpretation of data related to the organization's cybersecurity. This encompasses many activities, including monitoring network traffic, analyzing logs for unusual activities, and staying abreast of the latest threat intelligence feeds. The goal is to detect anomalies, potential security incidents, or indicators of compromise in real-time, allowing for swift response and mitigation. One key aspect of continuous monitoring is the ability to detect and respond to changes promptly. This proactive stance ensures that organizations can address potential vulnerabilities or security gaps before malicious actors can exploit them. In a rapidly evolving digital landscape, the ability to adapt quickly is a critical factor in maintaining a resilient cybersecurity posture. Continuous monitoring also aids compliance management by providing a mechanism to track adherence to security policies and regulatory requirements. Regular security controls and configuration assessments help organizations demonstrate compliance with industry standards and regulations. This mitigates the risk of regulatory penalties and reinforces the overall security posture.

Moreover, the insights gained from continuous monitoring contribute to informed decision-making. Organizations can allocate

resources judiciously, prioritize remediation efforts, and make strategic decisions to enhance their cybersecurity strategy by having a real-time understanding of the security landscape. This data-driven approach enables organizations to focus on areas of higher risk and allocate resources effectively. Continuous monitoring is a proactive and ongoing process crucial for maintaining a robust cybersecurity stance. By staying informed about changes in the target environment, organizations can adapt to evolving threats effectively. This approach enhances the ability to detect and respond to security incidents promptly and supports compliance management and informed decision-making in cybersecurity.

4. Result and Discussion

The study's findings reveal that certain requirements engineering (RE) techniques and tools, such as introspection, document analysis, and passive observation, may not be suitable for all four criteria: safety, utility, learnability, and usability. These methods create a separation between stakeholders and the RE process, hindering cooperation and a comprehensive understanding of stakeholders' needs. Group techniques like Joint Application Development (JAD) sessions, which involve active participation, can be perceived as risky, potentially hindering safety and openness in expressing concerns among stakeholders. Consequently, it is advisable to avoid using JAD sessions when stakeholders' safety is paramount.

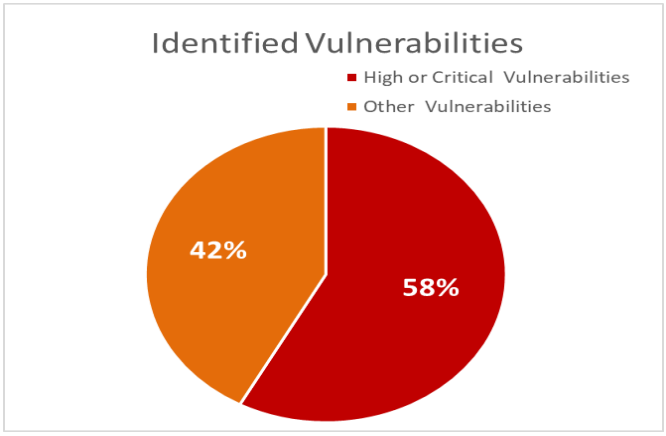

Figure 2: Identified vulnerabilities since 2018

Moreover, active observation, often associated with feeling unsafe, may impede the RE process as individuals tend to behave cautiously when aware of being observed. On the contrary, methods like interviews, questionnaires, user scenarios, card sorting, laddering, and prototyping, when conducted as standalone activities, are less likely to raise safety concerns among participants. Card sorting, laddering, and user scenario strategies are the most effective regarding stakeholder utility. These methods are designed to elicit knowledge, analyze issues, and determine the domain of potential solutions from the stakeholders' perspective, thereby maximizing their utility.

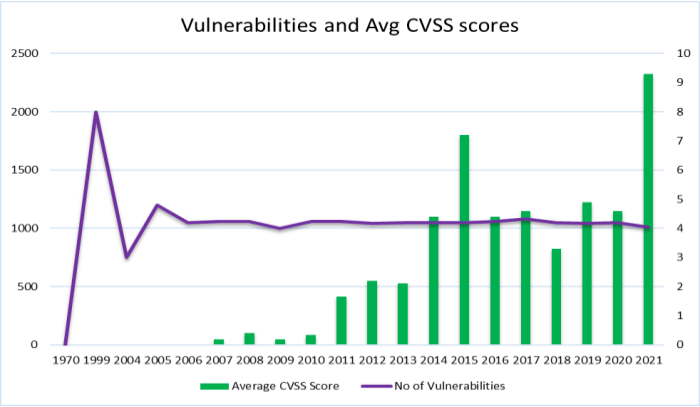

Figure 3: Vulnerabilities and average CVSS scores over various time frames

High stakeholder utility increases the likelihood of collaboration and improvement in the RE process. Semi-structured and unstructured interviews, prototypes, and JAD sessions are deemed most beneficial as they facilitate in-depth discussions about stakeholders' viewpoints on business requirements and potential solutions.

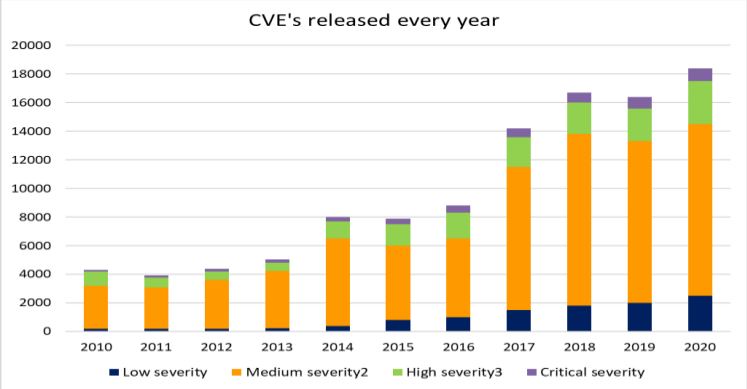

Figure 4: CVEs released every year

Figure 2 illustrates identified vulnerabilities since 2018. Figure 3. Vulnerabilities and average CVSS scores over various time frames. Figure 4 illustrates the CVEs released every year.

5. Conclusion

This paper emphasizes the significance of information-gathering techniques in fortifying organizations against cyber threats. By applying these techniques, organizations can collect vital system-level information, including details about the target operating system, network systems, active machines, and open/closed ports. Implementing best practices in information gathering serves as a robust defense, enhancing understanding and safeguarding network systems from potential hacker intrusions. Detailed insights into the target operating system's configuration and vulnerabilities can be gained through meticulous information gathering. Similarly, analyzing active running machines ensures the identification of authorized systems and the detection of any anomalies indicating unauthorized access. Assessing open and closed ports contributes to a comprehensive understanding of the network's security posture. Adopting effective information-gathering practices empowers organizations to proactively address vulnerabilities, mitigate risks, and secure critical infrastructure. As cybersecurity threats evolve, a proactive and informed approach to information gathering remains pivotal in defending against potential breaches.

Acknowledgment: The support of all my co-authors is highly appreciated.

Data Availability Statement: This study uses benchmark data available online to conduct the research. This is a fresh study done by the authors.

Funding Statement: There has been no funding obtained to help prepare this manuscript and research work.

Conflicts of Interest Statement: No conflicts of interest have been declared by the author(s). This is the authors' fresh work. Citations and references are mentioned as per the used information.

Ethics and Consent Statement: The consent has been obtained from the colleges during data collection and has received ethical approval and participant consent.

References

1. A. Yadav, A. Kumar, and V. Singh, "Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security," Artif. Intell. Rev., pp. 1–32, 2023.
2. K. M. Carley, "Social cybersecurity: an emerging science," Comput. Math. Organ. Theory, vol. 26, no. 4, pp. 365–381, 2020.
3. S. F. Aboelfotoh and N. A. Hikal, "A review of cyber-security measuring and assessment methods for modern enterprises," JOIV: International Journal on Informatics Visualization, vol. 3, no. 2, pp. 157–176, 2019.
4. G. Markowsky and L. Markowsky, "Visualizing Cybersecurity Events," in the 2013 International Conference on Security & Management, Las Vegas, Nevada, USA, 2013.
5. M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," IEEE Access, vol. 10, pp. 40281–40306, 2022.

6. I. P. A. E. Pratama and A. A. B. A. Wiradarma, “Open source intelligence testing using the owasp version 4 framework at the information gathering stage (case study: X company),” International Journal of Computer Network and Information Security, vol. 11, no. 7, pp. 8–12, 2019.
7. S. Kaushik, A. Bhutto, B. Pandey, “Efficient Information Gathering using NMAP and NBTSCAN: Case study on 172.19.19.0 IP Address,” Indian J. Sci. Technol., vol. 12, no. 28, pp. 1–13, 2019.
8. M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, “Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis,” IEEE Access, vol. 9, pp. 138509–138542, 2021.
9. J. Swartz, “Security systems for a mobile world,” Technol. Soc., vol. 25, no. 1, pp. 5–25, 2003.
10. J. Friedman and D. V. Hoffman, “Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses,” Information Knowledge Systems Management, vol. 7, no. 1–2, pp. 159–180, 2008.
11. P. Ghorbanzadeh, A. Shaddeli, R. Malekzadeh, and Z. Jahanbakhsh, “A survey of mobile database security threats and solutions for it,” in The 3rd International Conference on Information Sciences and Interaction Sciences, 2010.
12. I.-K. Lim, Y.-G. Park, and J.-K. Lee, “Design of security training system for individual users,” Wirel. Pers. Commun., vol. 90, no. 3, pp. 1105–1120, 2016.
13. C. J. Cremers, “The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols: Tool Paper,” in International conference on computer aided verification, Berlin, Heidelberg; Berlin Heidelberg: Springer, 2008, pp. 414–418.
14. S. N. Narayanan, A. Ganesan, K. Joshi, T. Oates, A. Joshi, and T. Finin, “Early detection of cybersecurity threats using collaborative cognition,” in 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), 2018.
15. H. Berger and A. Jones, “Cyber security & ethical hacking for SMEs,” in Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society, 2016.
16. A. Ahmed Chhipa et al., “Adaptive Neuro-fuzzy Inference System Based Maximum Power Tracking Controller for Variable Speed WECS”,” Energies, vol. 14, 2021.
17. A. K. Sharma et al., “Classification of Indian Classical Music with Time-Series Matching using Deep Learning”,” IEEE Access, vol. 9, pp. 102041–102052, 2021.
18. A. K. Sharma et al., “Dermatologist-Level Classification of Skin Cancer Using Cascaded Ensembling of Convolutional Neural Network and Handcrafted Features Based Deep Neural Network”,” IEEE Access, vol. 10, pp. 17920–17932, 2022.
19. A. K. Sinha, A. Shankar Hati, M. Benbouzid, and P. Chakrabarti, “ANN-based Pattern Recognition for Induction Motor Broken Rotor Bar Monitoring under Supply Frequency Regulation”,” Machines, vol. 9, 2021.
20. A. Magare, M. Lamin, and P. Chakrabarti, “Inherent Mapping Analysis of Agile Development Methodology through Design Thinking”,” Lecture Notes on Data Engineering and Communications Engineering, vol. 52, pp. 527–534, 2020.
21. D. Bhuva and S. Kumar, “Securing space cognitive communication with blockchain,” in 2023 IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW), 2023.
22. D. K. Sharma, B. Singh, M. Raja, R. Regin, and S. S. Rajest, “An Efficient Python Approach for Simulation of Poisson Distribution,” in 2021 7th International Conference on Advanced Computing and Communication Systems, 2021.
23. D. K. Sharma, B. Singh, R. Regin, R. Steffi, and M. K. Chakravarthi, “Efficient Classification for Neural Machines Interpretations based on Mathematical models,” in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021.
24. D. K. Sharma, N. A. Jalil, R. Regin, S. S. Rajest, R. K. Tummala, and Thangadurai, “Predicting network congestion with machine learning,” in 2021 2nd International Conference on Smart Electronics and Communication, 2021.
25. D. K. Srivastava and B. Roychoudhury, “Understanding the factors that influence adoption of privacy protection features in online social networks,” J. Glob. Inf. Technol. Manag., vol. 24, no. 3, pp. 164–182, 2021.
26. D. K. Srivastava and B. Roychoudhury, “Words are important: A textual content based identity resolution scheme across multiple online social networks,” Knowl. Based Syst., vol. 195, no. 105624, p. 105624, 2020.
27. D. R. Bhuva and S. Kumar, “A novel continuous authentication method using biometrics for IOT devices,” Internet of Things, vol. 24, no. 100927, p. 100927, 2023.
28. F. Arslan, B. Singh, D. K. Sharma, R. Regin, R. Steffi, and S. Suman Rajest, “Optimization technique approach to resolve food sustainability problems,” in 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021.
29. G. A. Ogunmola, B. Singh, D. K. Sharma, R. Regin, S. S. Rajest, and N. Singh, “Involvement of distance measure in assessing and resolving efficiency environmental obstacles,” in 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021.
30. G. K. Bhamre and S. S. Banait, “Parallelization of Multipattern Matching on GPU,” Communication & Soft Computing Science and Engineering, vol. 3, no. 3, pp. 24–28, 2014.

31. G. Kumawat, S. K. Vishwakarma, P. Chakrabarti, P. Chittora, T. Chakrabarti, and J. C.-W. Lin, “Prognosis of cervical cancer disease by applying machine learning techniques,” J. Circuits Syst. Comput., vol. 32, no. 01, 2023.
32. K. Shah, P. Laxkar, and P. Chakrabarti, “A hypothesis on ideal Artificial Intelligence and associated wrong implications”,” Advances in Intelligent Systems and Computing, vol. 989, pp. 283–294, 2020.
33. K. Sharma, B. Singh, E. Herman, R. Regine, S. S. Rajest, and V. P. Mishra, “Maximum information measure policies in reinforcement learning with deep energy-based model,” in 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021.
34. L. W. Santoso and I. Widjanadi, “The application of New Information Economics Method on distribution company to improve the efficiency and effectiveness of performance”,” International Journal of Engineering and Manufacturing, vol. 6, no. 5, 2016.
35. L. W. Santoso, “Cloud technology: Opportunities for cybercriminals and security challenges,” in 2019 Twelfth International Conference on Ubi-Media Computing (Ubi-Media), 2019.
36. M. Akbar, I. Ahmad, M. Mirza, M. Ali, and P. Barmavatu, “Enhanced authentication for de-duplication of big data on cloud storage system using machine learning approach,” Cluster Comput., 2023.
37. M. Awais, A. Bhuva, D. Bhuva, S. Fatima, and T. Sadiq, “Optimized DEC: An effective cough detection framework using optimal weighted Features-aided deep Ensemble classifier for COVID-19,” Biomed. Signal Process. Control, p. 105026, 2023.
38. M. Farooq and M. Khan, “Signature-Based Intrusion Detection System in Wireless 6G IoT Networks,” Journal on Internet of Things, vol. 4, no. 3, pp. 155–168, 2023, doi: https://doi.org/10.32604/jiot.2022.039271.
39. M. Farooq, “Artificial Intelligence-Based Approach on Cybersecurity Challenges and Opportunities in The Internet of Things & Edge Computing Devices,” International Journal of Engineering and Computer Science, vol. 12, no. 07, pp. 25763–25768, Jul. 2023, doi: https://doi.org/10.18535/ijecs/v12i07.4744.
40. N. Priyadarshi, A. K. Bhoi, A. K. Sharma, P. K. Mallick, and P. Chakrabarti, “An efficient fuzzy logic control-based soft computing technique for grid-tied photovoltaic system”,” Advances in Intelligent Systems and Computing, vol. 1040, pp. 131–140, 2020.
41. P. Chakrabarti, S. Bane, B. Satpathy, M. Goh, B. N. Datta, and T. Chakrabarti, “Compound Poisson Process and its Applications in Business”,” Lecture Notes in Electrical Engineering, vol. 601, pp. 678–685, 2020.
42. P. Chakrabarti, T. Chakrabarti, M. Sharma, D. Atre, and K. B. Pai, “Quantification of Thought Analysis of Alcohol-addicted persons and memory loss of patients suffering from stage-4 liver cancer”,” Advances in Intelligent Systems and Computing, vol. 1053, pp. 1099–1105, 2020.
43. R. Angeline, S. Aarthi, R. Regin, and S. S. Rajest, “Dynamic intelligence-driven engineering flooding attack prediction using ensemble learning,” in Advances in Artificial and Human Intelligence in the Modern Era, IGI Global, 2023, pp. 109–124.
44. R. Oak, M. Du, D. Yan, H. Takawale, and I. Amit, “Malware detection on highly imbalanced data through sequence modeling,” in Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security - AISec’19, 2019.
45. R. Regin, A. A. Khanna, V. Krishnan, M. Gupta, S. Rubin Bose, and S. S. Rajest, “Information design and unifying approach for secured data sharing using attribute-based access control mechanisms,” in Recent Developments in Machine and Human Intelligence, IGI Global, pp. 256–276, 2023.
46. S. Praveen Kumar Sharma, “Common fixed point for weakly compatible maps in intuitionistic fuzzy metric spaces using property (S-B)”,” Journal of Non-linear Analysis Optimization and Theory, vol. 5, no. 2, pp. 105–117, 2014.
47. S. Praveen Kumar Sharma, “Common Fixed Point Theorems for Six Self Maps in FM-Spaces Using Common Limit in Range Concerning Two Pairs of Products of Two Different Self-maps”,” Revista Geintec-Gestao Inovacao E Tecnologias, vol. 11, no. 4, pp. 5634–5642, 2021.
48. S. S. Banait and S. S. Sane, “Result Analysis for Instance and Feature Selection in Big Data Environment,” “International Journal for Research in Engineering Application & Management (IJREAM), vol. 8, no. 2, pp. 210–215, 2022.
49. S. Sharma and P. K. Sharma, “A study of SIQR model with Holling type–II incidence rate,” Malaya J. Mat., vol. 9, no. 1, pp. 305–311, 2021