Incident Response Simulation Framework

Aananaya Mathur
AIT-CSE (Information Security)
Chandigarh University
Gharuan, Punjab, India
anya.mathur18@gmail.com

Geetika Jain
AIT-CSE(Information Security)
Chandigarh University
Gharuan, Punjab, India
geetikagargnm@gmail.com

Harsh Saroop
AIT-CSE(Information Security)
Chandigarh University
Gharuan, Punjab, India
harshsaroopraja@gmail.com

Lagan Verma
AIT-CSE(Information Security)
Chandigarh University
Gharuan, Punjab, India
laganverma3515@gmail.com

Ms. Sheetal Laroiya
Assistant Professor
Chandigarh University
Gharuan, Punjab, India
sheetal.e15433@cumail.in

***Abstract*— Incident response is a pivotal security role in organizations that aimed to manage incidents quickly and economically. Cybersecurity Incident Response is a valuable development in the mitigation and operational security and data protection methods to safeguard employees and their assets. Cybersecurity awareness training is a powerful approach that leverage companies to cultivate employees into developing their knowledge and awareness of best practices and strategies for safeguarding sensitive data. Incident response is an emerging field due to the exceptional rise in the security breaches. The organizations need to implement such incident responses for the data breaches. The operational teams should be equipped with the hands-on experience of the incidents. The real-world scenarios must be used as a method to enhance the knowledge of the security team. The proposed system responds to such security demands generating an environment to test the security architecture, measure, track and report Cybersecurity KPIs as overall threat exposure to reduce exposure risk. The system is an educative framework for giving a real-world experience to the users and also test their ability and agility to respond to the incidents in the given time and correctly.**

Keywords—Incident response, Cybersecurity, data breaches, security

I. INTRODUCTION

A cyber-attack is a vicious and purposeful attempt by either an individual or an organization to compromise the information system of another individual or organization [1]. In the recent years there has been a sharp increase in the frequency of cyber-attacks across the world. The digitization of the world is increasing the risk of these attacks. The cyber-attacks can be very lethal because the primary focus of the attacks is to gather the information of the clients and use it as and when required. The digitalize world gives power to those who have abundance of data. The cyber-attacks main focus is to gather all those data and disrupt the normal functioning of the organization and the users. The cyber-attacks can only be mitigated and contained with effective incident response plans. Incident response is the emerging field which is strategic and organized that manages security incidents. The frequency of cyber-attacks is increasing day by day and it has become the world's necessity. A cyber-attack can cause huge damage to an organization data and assets of an organization. The incident response is used to seek to limit damage and repair breached vulnerabilities in systems. Incident response outlines a structured process and breaks it down into a series of phases for handling security events [2]. The incident response methodologies vary on the basis of the need of the organization. The most renown frameworks include: NIST Framework, CERT, ITIL, TTP, etc. These frameworks are the set of guidelines, standards, and best practices that should be adhered by organizations as standards to keep their incident response plan up to date with the growing vulnerabilities and cyber-attacks. The incident response plans and framework should be agile because it plays an essential role in forming the security foundation of any organization. The Cybersecurity incident response process consists of a set of coordinated actions, procedures aimed to identify, analyze, and counter potential security threats, thereby ensuring these attacks have minimal impact and facilitates rapid recovery. The incident response teams should be capable to adhere to the international guidelines and perform security operations in their organizations according to the framework adopted.

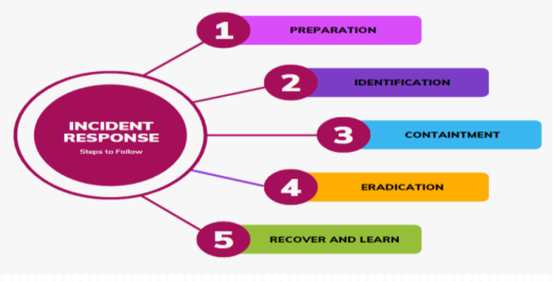


Figure 1: Incident response Steps

Educating individuals to protect their assets is the crucial need of the hour and should be taken seriously by all the individuals and their organizations. Attackers presently use sophisticated tactics to trick the employees into the web of attacks, Understanding the tactics, tricks and procedures of the attackers should be the main priority of the incident response team to eradicate any threat to their organization or asset. Additionally, appreciation of the potential consequences of falling victim to these attacks can motivate individuals to take necessary precautions to protect their sensitive information [3]. This paper introduces the concept of educating individuals about how cyber-attacks takes place and what steps should be taken to mitigate the threats. This paper focuses on developing a simulation framework for incident responses that can be used as a tool to educate the users about the attacks and how to respond to these attacks. In the upcoming section of the paper, we will discuss our simulation framework by incorporating background in the paper that introduces the readers to the in-depth need for this paper. Furthermore, another section will provide an outline of the simulation framework designed for the individuals and the organizations to enhance their incident response skills.

II. BACKGROUND

The field of Cybersecurity comprises of the practices and the actions that are related to manage security risks, processes and incident response processes. These processes should be implemented by organizations to safeguard the confidentiality, integrity and availability of the organizations assets. The number of cyber-attacks are increasing day by day. The exposure of these digital devices to the world is a necessity, however, the attacker ceases these opportunities to breach the security posture of the organization or the individual's security features. The assets might include any valuable information like digital content owned by either an organization or an individual that is distinctly identifiable and holds value to them. The information used by the hacker can be gathered through digital technologies, IOT embedded systems, multi-media content, audio, videos, websites etc. Organizations must implement a comprehensive security strategy that comprises of skilled personnel, policies, established processes and procedures and user training to safeguard their assets and protect their valuable information against cyber-attacks.

Incident Response is the term that is used in the Cybersecurity domain which is a well-defined approach to identify, control, and eliminate cyber threats and also to reinstate business operations as quickly as possible. The central focus of the incident response team is to mitigate the risk and recover the loss in both quantitative and qualitative manner. Cybersecurity incidents are unexpected or unwanted cyber incidents that have a high likelihood of disrupting business operations [4]. The existence of individuals, procedures, and data resources enhances the likelihood of a cyber event and makes it more susceptible to cyber-attacks. Incident Response is the core areas of an organization's Cybersecurity plans. The company with the most reliable techniques and tactics for mitigating and avoiding the risks associated with the cyber-attacks are the companies with more customer base and customer satisfaction. The incidents disrupts normal functioning of the organization and presents those organizations as failures in the business realm.

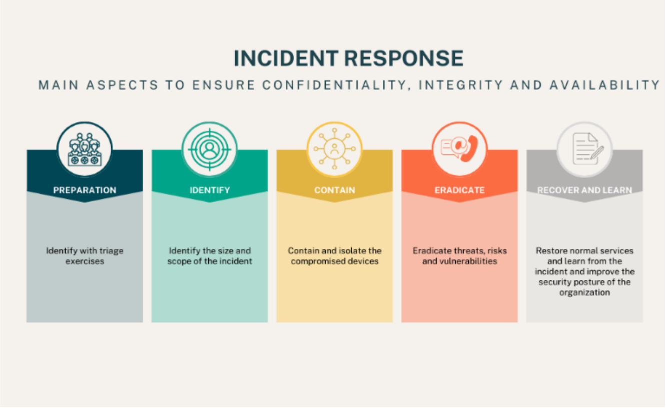

INCIDENT RESPONSE
MAIN ASPECTS TO ENSURE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY
PREPARATION
Identify with triage exercises
IDENTIFY
Identify the size and scope of the incident
CONTAIN
Contain and isolate the compromised devices
ERADICATE
Eradicate threats, risks and vulnerabilities
RECOVER AND LEARN
Restore normal services and learn from the incident and improve the security posture of the organization

Figure2: Incident Response Plan

To effectively combat Cybersecurity attacks and data breaches, individuals should be equipped with knowledge of various Cybersecurity attacks and vulnerabilities identified by resources such as CVEs , OWASP Top 10, etc. Few of the attacks are discussed below:

1. DDOS Attack: DDOS stands for Distributed Denial of Service Attack which is a vicious attempt to disrupt the regular operations and normal functioning of the targeted system or network by overwhelming the target system or network with a flood of Internet traffic.
2. Man in the middle attack: A Man-in-the-Middle attack occurs when a malicious actor interrupts communication between a client and a server without their knowledge. The attacker impersonates both the client and the server, potentially stealing information.[5]
3. Phishing Attacks: Phishing attacks are the most common attacks in Cybersecurity. It is the way of sending fraudulent emails as deceptive messages that are crafted which seems genuine and to appear from a reliable source to trick recipients into revealing

personal information or clicking malicious links. Phishing emails are a form of social engineering attack used to trick users into clicking malicious links and gaining information from the user by either directly downloading malware onto the systems, or re-directing them to another fake website designed to steal information.

4. Password Attacks: One of the most favored attacks among hackers is the password attack. The technique involves obtaining passwords by encryption or decryption of the password by illegitimate means. Password attacks do not require hacker to indulge into complex hacking technique; however, they can obtain information through simpler methods like social engineering or observing user behavior to obtain the password of the user.

5. SQL Injection Attack: Structured Query Language is a robust computer programming language crafted to generate, manipulate, oversee, and fetch data from relational databases. An SQL Injection attack involves injecting malicious code into the queries generated in the database for data retrieval, manipulation and storage. The SQL Injection manipulates the database at the back-end which may result in unauthorized access to sensitive data , deletion of data, and direct attack on the database itself.

The cyber-attacks listed above are some common attacks that are being used every day which poses high security threats to the organization and also as an individual. This paper works on designing a simulation framework that can help in maintaining the integrity of the organization and help in protecting the assets of the company as well as the customers. The incident response framework is adapted and merged from various frameworks that incorporates industry standards and best practices, some of the frameworks are listed below:

1. NIST Incident Response: The National Institute of Standards and Technology (NIST) is an agency within the United States Department of Commerce. It oversees standards and measurement methodologies for information technology, including information security NIST framework emphasizes an ongoing learning process and continuous improvement. It encourages organizations to learn how to best protect theselves and adapt their response strategies over time.

2. ISO 27,001 Framework: The International Electrotechnical Commission (IEC) collaborated to create the ISO/IEC 27001 standard with The International Organization for Standardization (ISO) [6]. The ISO/IEC 27001 framework promotes best practices and information security controls to effectively manage information security risks. It is also responsible for establishing requirements for implementing, maintaining and improving an Information Security Management Systems over time. This framework helps organizations of all sizes to protect their data in structured and economical manner.

3. COBIT 2019: The Control Objectives for Information and Related Technology framework was developed by the Information System Audit and Control Association (ISACA). COBIT 2019 provides guidelines and directions to the organizations towards the administration of their IT infrastructure that supports business operations and processes [7]. The primary objective of the framework is to issue an all over view of the administration of the IT systems and follow a comprehensive approach.

The frameworks helps the organizations to safeguard their cyberspace. The incident response simulation frameworks play a critical role in accomplishing the security goals of an organization by providing an overview of the incident responses taken by the client and the admin to safeguard the cyberspace of the organization.

III. PROPOSED METHODOLOGY

The proposed system provides a basic simulation framework for the incident response of the User Behavior Analytics. The focus of the paper is on how the UBA attack works and what are the incident response techniques that can be used by an organization or the IT team of the organization to prevent these attacks. The paper proposes the basic framework for the simulation and provides a diligent product alongside which helps in educating and training the IT teams of the organization.

User Behavior Analytics (UBA) involves the continuous tracking, monitoring, collection and analysis of user data and activities within systems. It helps in identifying abnormal user behavior by tracking the advances used by the user and determines if the abnormality is a threat to the organization and restores the operation using statistical analysis and predefined correlation rules.

The proposed system is a simulation framework for user behaviour analytics, which recognizes the importance of users as prospect of internal threats. The system proposes solutions for abnormalities in the login systems used by the users and addresses prevalent problems that arise from them.

Our comprehensive approach lies on the two primary used operating systems: Windows and Linux. The project is a successful implementation of the two other systems that includes the operations of UEBA i.e. User Entity and Behaviour Analytics.

The system incorporates a login system for the monitoring of the user behaviour. The simulation starts with a welcome page that provides the user an interface to communicate with the system and ask the user to click on the start simulation button to begin the simulation for educating and training users on how to respond to the provided cyber-attack.

The simulation leverages various python libraries that deliver its core functionalities which includes several key components:

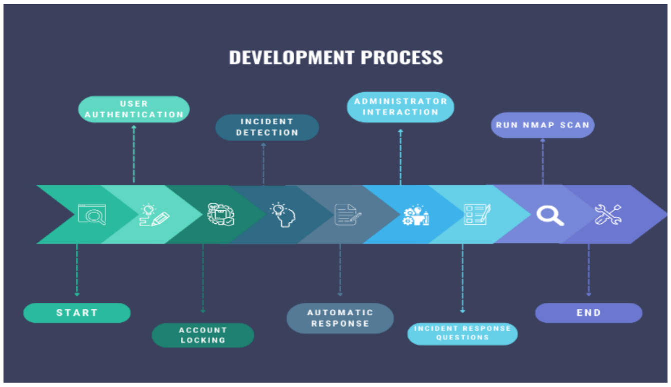
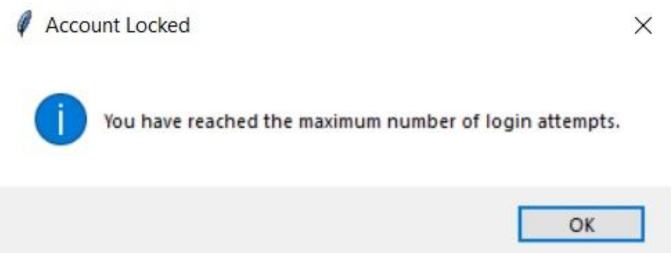


Figure 3: Development Process

Login Authentication: The user clicks on the start simulation button and is directed towards an authentication system which is mainly used by multiple organizations called the login system. The user signs in the system by the provided credentials. If the user signs in the system in the given three attempts, the user is allowed access to the system, else the system monitors this as an attempt to breach the authentication system.

Failed Login Tracking: The UBA system is used for tracking and monitoring the attempts for breach in the authentication system. The system monitors and records the number of failed logins attempts, and the timestamps of each failed login attempt. This helps in monitoring the frequency and timing of login attempts that help the IT personnel to understand the potential security threats like brute force attack etc.

Account Locking: When the client exceeds the predefined threshold of failed login attempts, the login button is disabled, triggering the account locking mechanism. The user's account is then locked for a random duration to prevent further login attempts in due course of time, thereby enhancing security by implementing a risk mitigation technique for unauthorized access.


Account Locked

You have reached the maximum number of login attempts.

Figure 4: Account Locked

Incident Recording: When suspicious activity, such as multiple failed login attempts, is detected, an incident or an event information is logged with details including timestamp, IP address, username used, password used, action generated, and all additional information. This stage records a history log of security events, aiding in post-incident analysis, forensic investigation and compliance reporting.

Alert System: The alert system is an additional part of the admin panel where a sound alert is generated for a stipulated time untthe admin prompts it to stop, assisting in addressing the immediate effect of the discovered incident.

Email System: To enhance alerting and security, the authentication system generates automated and instant mail to the concerned department heads, the admin is informed about the issue in the security posture, informing them about the current scenario.

Overall, the functions together act as an educating system on the windows operating system. The functionalities, however extends towards the usage of Kali Linux as a useful tool for the testing and education purposes. The Kali Linux operating system simulation offers multitude of questions to answer on how to respond to the incident taking place and also show the speciality of Kali Linux tools.

The Linux simulation also offers the same simulation of User Behavior Analytics to the user; however, the user is more engaged with the simulation with the adoption of questionnaire technique.

The participants following a successful login encounters a series of questions designed to assess the fundamental concepts and procedures outlined in the incident response plan. This should be the priority for the IT and security teams to effectively strengthen organization's security posture.

After successful compilation of the incident response questions, the client is given option to execute a network scan using NMAP tool. The health of the system is an integral part of any incident response plan. This tool helps proactively investigate the phases of incident response.

The NMAP tool is used to scan the IP of the traced IP address and determines the open ports and services of the current system, thereby, inducing the importance of updates and patch management in the client and admin incident response plan.

Additional features of the Proposed System are:

- Account Locking Mechanism
- Incident Recording
- Visualization of Login Activity
- Integration with External tools

IV. DISCUSSION

Our proposal for an incident response simulation framework is a promising approach towards educating the team members of the organization, beginning from the novice learners who have no clue about the security implications of the system used, to brushing up on the basic concepts and fundamentals for advanced learner. The learners can visualize the concept of UBA through our incident response simulation framework that provides the client insights about the most common but most overlooked series of threats to the organization. The simulation offers the most important and general ways of defending against user attacks. The admin and client portal are differentiated using Tkinter library of Python to help the audience visualize the arena of both the user and the admin side. The features such as account locking, incident recording etc. are sections of the incident response plans which are standardized for the organizations to follow. The proposal is built for both the systems offering different plan structure to follow. The use of two different operating systems helps the user to determine the effectiveness of operating systems as well as the vulnerabilities of the system. The proposed system offers a number of benefits such as:

- Transparency
- Auditability
- Accountability

The simulation is transparent for the user to see the transactions going between the system and the admin. The report generation on every failed attempt and the graph with the timestamp of the failed attempt encourages governance through the system.

The system majorly focuses on the authentication system at the time of the research. However, the team is constantly researching more advanced versions of user behavior abnormalities for further advancement of the project.

The additional features that can be integrated in the later stages can be as followed:

User Training Modules: Deep and interactive modules within the GUI can be integrated for the user to practice best cybersecurity techniques and procedures.

The integration of machine learning modules for real time threat detection can help in making the system more robust and helpful for education purposes.

The system for simulation can be designed with a more scalable approach, which would be able to handle increasing number of users simultaneously.

The incident response plan for the simulation framework offers a comprehensive and robust platform for cybersecurity training and user interaction with the system for both the novice and advanced learner, thereby, assisting the organization in safeguarding their digital assets and protecting against cyber threats

V. CONCLUSION

The digital world solely relies on the data that is stored in the systems, on the network, the cloud etc. The importance of this data arises the importance of the plans and procedures that need to be a part of the organization safety structure for smooth business operations. The incident response plan is the need of the hour, applicable to all sizes, from the smallest to the high-income enterprises that require their data to be secured and no compromise in their business operations.

Through the proposed system organizations can enhance the ever-evolving threat landscape in cyberspace, by educating teams on the given platforms and providing hands-on training. The realistic simulation environment which incorporates the threat landscape can provide and insight into the ongoing abnormalities in the system or can use the experience in the future. The employees take proactive security measures and are vigilant enough to detect and respond to the event immediately before they escalate into a security breach. The project offers an intuitive platform for cybersecurity training. Users can interact with the system, learn the best practices and understand the implications of their actions in a simulated environment. This promotes security awareness and empower individuals to make informed decisions in real world scenarios.

REFERENCES

[1] Cyber Attack - What Are Common Cyberthreats? Cisco

[2] D. Schlette, M. Caselli and G. Pernul, "A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2525-2556, Fourthquarter 2021, doi: 10.1109/COMST.2021.3117338. keywords: {Security;Standards;Organizations;Tutorials;NIST;Digital forensics;Collaboration;Cyber threat intelligence;incident response;standardization;playbook format},

[3] A Cyberattack Simulation for Teaching Cybersecurity Christopher Scherb1 ∗ , Luc Bryan Heitz1† , Frank Grimberg1‡ , Hermann Grieder1§ , and Marcel Maurer2¶R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[4] Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities Ayesha Naseer a, Humza Naseer b, Atif Ahmad c, Sean B Maynard c, Adil Masood Siddiqui d

[5] CYBER ATTACKS AND ITS DIFFERENT TYPES Jibi Mariam Biju1, Neethu Gopal2, Anju J Prakash3 1,2Mtech, CSE Department, Sree Buddha College of Engineering, Kerala, India 3Assistant Professor, CSE Department, Sree Buddha College of Engineering, Kerala, India

[6] Industry 4.0 data security: A cybersecurity frameworks review pane lMarion Toussaint [a], Sylvère Krima [b], Hervé Panetto ¨ Université de Lorraine, CNRS, CRAN, 54000 Nancy, France Georgetown University, Washington, DC, 20057, USA

[7] A Dynamic and Adaptive Cybersecurity Governance Framework by Henock Mulugeta Melaku