Jehan Turki Nasraddin, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 14, Issue 10, October 2024, pp 63-72

RESEARCH ARTICLE OPEN ACCESS

Detection of Malicious Privileged Access Using a Rule-Based Approach

Jehan Turki Nasraddin
Eynas Hassan Balkhair
A research project submitted for the requirements of the degree ofExecutive Master of Cybersecurity

Dr. Manar Salamh

ABSTRACT
Privilege insiders are harder to detect by organizations. An organization's systems are subjected to threats that will affect missions, assets, and individuals of the organization. Many organizations affected by threats over a year. This paper modeled the path of actors that aims to publish and share sensitive data of the company such as files to unauthorized users by insider attack by using State Transition Diagram and developed detection of the modeled insider attack paths using the rule-based approach. There are seventy-seven attack steps that can be taken to achieve goals of publishing and sharing sensitive company files which are done by an insider attack. After deep studying of the attacks steps, the designed diagram has layered the attack steps based on analysis and aggregated them to five groups.
This paper also uses offline analysis, which use the log file after the attack occurred, publish process is not affected in offline analysis. Rules and pseudocode are explained in detail.
Key Word: insider attack, rule-based, attack step, offline analysis

---

Date of Submission: 08-10-2024 Date of acceptance: 21-10-2024

I. Introduction

Nowadays daily hacking between privileged insiders. Privileged insider has a wide knowledge and access to corporate information systems. Unauthorized usage of privileged users could cause massive damage to the corporate by exploiting its access rights [1]. A corporate could use different terms and tools to mitigate the risk of privileged insider attack. One of the most beneficial ways to mitigate insider attack risk is using security controls. Security controls are administrative, operational, and physical controls. The organization can implement one or more security control based on the risk and how the organization will address it. Administrative or (Management) security control helps implement a secure environment by providing guidance, rules, and procedures. Operational control is the implementation of access controls, authentication, and security concerns that are applied to the corporate information system and network. Physical security controls are the protection of the corporate system from physical threats that affect the organization's operations or impact confidentiality, integrity, or availability [2].

Organization information systems can be subject to threats that will affect missions, operations, reputation, assets, individuals, other organizations, and the nation, to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by the system. Threats to information and information systems include attacks, environmental disruptions, human or machine errors resulting in great harm to national and economic security. Therefore, administrators need to manage the information security risks associated with the operation and use of information systems that support an organization's mission and business functions.

According to NIST-SP 800-39, information security risk management is the process of collecting the decisions of responsible individuals and groups within corporate about strategic planning, oversight, management, and day-to-day operations to provide risk response measures to adequately protect the missions and business processes [3].

Privilege is known as the access granted by people within a corporate, such as employees, contractors, or business associates, to information about the organization's security practices, data, and information systems. The privileged insiders are those who have the legitimate right and corporate trust to overcome the security controls to harm the organization's assets [4].

Insider risk is the most important cyber

threat the organization cannot ignore [5]. The damage caused by insider attacks predominantly has a higher damage rate than the outsider attacks. Privilege insiders could steal company intellectual property, disable business operations that pose significant harm to the company and affect its system confidentiality, integrity, availability, damage its reputation, and lose its competitive advantage.

Many organizations have been impacted by insider threats over years. In 2017, an employee in Bupa was able to extract the personal information of 547,000 Bupa Global customers through Bupa's customer relationship management system (SWAN), which holds customer records relating to 1.5 million people. The employee sent bulk data reports to his email account and offered them for sale on the dark web. Bupa was fined £175,000 by the Information Commissioner's Office (ICO) Because of neglecting the implementation of security measures to protect the personal information of customers [6].

In September 2018 an employee in Cisco gained unauthorized access to the company's cloud infrastructure and used malicious code that eresed more than four hundred virtual machines used for Cisco's WebEx Teams application. This result in approximately 16,000 users of WebEx being unable to access their accounts for two weeks. Cisco lost $1.4 million to audit the infrastructure and to fix the damage that happened. In addition, pays $1 million in restitution to affected users [7].

NIST and ISO standards had produced controls to control privileged access in organizations. ISO 27001 has published Annex A.9 to restrict access to information and information processing facilities, and to ensure the user has access only to the information relevant to his role. A sub-control of A.9 is A.9.2 and 9.2.3, their objectives are to prevent unauthorized access, guarantee the user is authorized to access systems, and manage the privileged access rights [8]. (NIST) had published NIST Special Publication 800- 53 Security and Privacy Controls for Federal Information Systems and Organizations. The publication has discussed the AC-2, AC-3, AC-6, and CM-5 controls which they used to protect, monitor, and audit access of privileged accounts [9].

Detecting unauthorized access has attracted the interest of researchers in discovering modern methods and approaches. In a past study, in 2012 a proactive privileged insider detection system was proposed to depend on a graph and psychological approach [10]. In 2015 two famous approaches were proposed. The first approach is a probabilistic approach to detect privileged insiders by using event correlation and log analysis [11]. The second approach is an access control technique based on behavior that integrates the machine learning techniques against privileged insider detection in big data analytics [12]. Based on research, between 2017 to 2021 a various detection approaches were used, machine learning, rule-based, behavior modeling, and anomaly detection. In 2017 a detection method was produced using a tree-structure profiling approach [13]. In 2018, a threat detection method was produced using a deep neural network (DNN) [14]. Recently, research in 2020 deduce machine learning-based system for user-centered insider threat detection [15], A research in 2021, has presented an unsupervised learning-based anomaly detection approach for insider threat detection [16].

Corporates need to limit and mitigate the possibility of insider malicious attacks and avoid the harm it causes, impact business functionalities, steals trade secrets, and pose reputation damage, financial loss.

The logs can help on improving the performance of the system and network. In addition, logs record the user activity and provide data used in malicious activity investigation [17].

Event logs stores event type, source, category, ID, date-time, user, computer, description, primary username, primary logon ID and client domain of any evet occurred (Kent & Souppaya, 2006) [18]. The proposed method will combine the rule-based method and logs analysis for detecting insider threats.

1.1 Problem Statement

The privilege insiders are hard to detect by organizations. Nowadays, privileged insider attacks are posing a huge impact on organizations. The breached data by insider attacks raised 200% from 2018 to 2019 [18] and 68% of organizations are moderately vulnerable to insider threats. The organizations are exposed to insider attacks due to insufficient knowledge of insider threats impact, negligence of implementing good security controls or implementing weak security controls, insufficient user's authentication, and inadequate user behavior monitoring [19].

1.2 Objectives

The objectives of the proposed method are to provide real-time detection of insider attacks for decreasing overall organizational risk, by modeling attack steps and implementing rules for detection. Implementing this method will assist the organizations in detection of the insider threat before occurring.

1.3 Methodology

1. Conduct a literature review of current approaches and techniques for detecting malicious privileged access.
2. Developing a representation model for detecting malicious privileged access using state

transition diagram and defining the rules to filter the insiders' attacks using the rule-based methods.
3. Testing the defined method.
4. Evaluate the method.

1.4 Ethical considerations, if applicable

A puplished dataset will be used in this case study. The intigrity and availability of the dataset will have higher attention from our side.

1.5 Expected deliverables (Technical artifact)

Through the logs analysis and rule-based method used, accurate real-time insider detection will be implemented.

II. Background and Review of Related Work

2.1 Literature Review

Previous research showed that insiders are classified under three categories: masquerader, traitor, and unintentional perpetrator. Computer Emergency Response Team (CERT) has defined the masquerader they often use stolen credentials or an authorized user's computer that is comprised. While the traitors are the privileged user who negatively exploits their legitimate access to the organization's network, system, and data to affect confidentiality, integrity, or availability. And the human error accorded by an authorized employee known as the unintentional perpetrator [20].

This has also been explored in prior studies by [21] that classified the malicious insider under two categories: traitors and masqueraders. This paper is not focused on the human error classification and only gave attention to the other two. As mentioned, the classification could be made based on the knowledge amount both types have or the intent of the user's action. Under knowledge classification, the traitors have full knowledge of the used system, and the masquerade has less knowledge. Under the user action intent classification, the masquerader and traitors are following the same intent. While there is an unintentional preparator as mentioned in the first survey who not intended to do a malicious activity.

This section presents a review of the literature on USTAT. It is a real-time intrusion detection tool proposed by Phillip A. Porras, and it is a State Transition Analysis Tool for UNIX. It is based on the rule-based penetration identification and represents the computer presentation as a sequence of state changes from an initial system state to a target compromised state. The state on the diagram is a group of all system data that are volatile, permanent, and semi-permanent stored at a specific time.

In addition, audit data is the most popular data for the intrusion detection system. The audit trail refers to the audit records of all activities stored in the system in chronological order, the ability is available to manually edit the audit data and detect the abnormal activities. STAT used the audit trails created by audit collection mechanisms of the target operating system.

The rule-based identification tools have two known issues that have been solved by USTAT. The presentation requires a deep understanding of the audit collection mechanism by an experienced person who works with an intrusion detection system. Also, there could be several different audit record sequences for the same scenario, that pose an issue in the representation of penetrations based on pattern matching rules to the audit records.

To overcome the above issues, the USTAT had solved both issues by implementing the higher-level audit record independent representation of penetration scenarios and facilitating the process of the rule-based creation and update [22].

Several theories have been proposed to indicate the detection methods, some focusing on logs analysis, others on machine learning.

In [23] machine learning is used in dynamic malware detection, and the detection issues are either anomaly detection or classification.

Because the threats are available even with the smart systems, the large security operations centers have moved to deploy endpoint-based sensors which provide deeper visibility into low-level events across their enterprises. The experiment has three steps to detect the attack. The first step is to describe the audit log types and settings of the behavior that will be recorded. The second is to describe the effort that will be provided to collect the real enterprise audit log using these settings and set of drivers' samples whether it is malicious or benign. Finally, decide which binaries are malicious or not for using them in the training and testing the proposed detection approach.

To collect windows audit logs the defining types of the system object such as registry key, files, or network events are required, and the type of access must be recorded and monitored.

The results of the experimental dataset consist of 32,078 samples and 6,898,953 unique extracted features. Out of the samples is 17,399 are benign, and 14,679 are malicious. audit logs are from binaries executed in CuckooBox is 20,362, and 11,716 are Invincea's enterprise four-minute windowed audit logs.

For the event log analysis, the analyzing systems' failure behavior was benefiting from it. The relation between failure and event logs is that the system interface is contained by the failures ellipse and the event logs report a subset of errors. The rule-based logging was applied to two software to

discover logs' capability for detection [24].

In addition to the use of the rule-based framework, a novel approach was proposed for detecting intrusion in wireless sensor networks, to detect routing attacks the designed rules applied for detection by collected data validation [25].

A series of recent studies has indicated how the attack works and what are the activities conducted. The attack tree is described in [26] to produce an approach for identifying the expected daily work and the malicious attacks. The attack tree could be extended to define the possible sequence of activities to achieve the objective as the root of the tree define the attack objective, which either is conducting daily workload or conducting the malicious attack.

The branches of the root define the steps taken to achieve the objective. Each node represents a user activity or a monitoring tool activity. Each user will have his tree to represent the expected activity. All nodes preserve the event occurring time and more attributes, such as logon, logoff or USB devise nodes save the computer used for conducting event's information.

If a new activity is observed, the system will decide whether it is a normal or malicious activity by comparing the activity and the defined observation, and deciding which activity branch this chain of the event belongs to. The system also should determine the similarity between the observed branch and the existing branch. The tree will be extended in case there is a partial match between the two branches. And if they are similar the tree will remain the same. In case the observed branch does not exist in the tree and there is some attribute similarity, the system will calculate branch similarity between each existing branch and observed branch.

The dataset defined the logon, logoff of machines, sending emails, accessing files and websites, and using USB devices. During the dataset time (a year and a half) the scenario has been conducted on or more employees performing malicious activity.

The activity tree is defined for one user and one role which consists of 27 possible paths for conducting the normal activity. While the activity tree for conducting malicious activity is 7 paths out of 8 and 6 of them have seen USB device usage. In comparison with the normal activities, the user has never been observed using USB devices. This concept should be extended to support thousand of insider-threat case scenarios and to identify the computational complexity of extending the tree-profiling concept when dealing with a wider range of activities and attributes that are available from synthetic data.

The paper [27] supports the idea of the attack tree and had constructed the attack-pattern tree for intellectual property (IP) theft. The attack pattern will be used within a machine learning-based threat detection prototype. The attack-pattern tree will define the attack step and the most prevalent path for each attack type, these attack steps are related to anomaly metics. The de-constructing of the case studies started by assessing the attack step, then grouping the steps that have a similar meaning. After collecting and modeling enough attacks, the attack steps will be established. Defining the attack steps is the first step to identifying attack patterns. Attack steps in the attack-pattern tree are colored green as it can be detected by the machines and red-colored where human detection is required, and the tree is also classified into five different classes, as they are normal behavior, covering tracks, weaponization, attack, and outcome.

When the attack-patten observed, the research intended to define how attack steps could be identified through detection capabilities. The prototype detection system had constructed the anomalies based on each proposed metric, which indicates the amount of deviation observed. There are two anomaly metrics used. Metric is either the anomalies based on user action in respect to individual activities, or the anomalies based on how the user acts across different activities.

As described in the research, the steps and the value gained from each step of stealing sensitive IP are described as follows: for gathering intelligence the insider threat may determine which of their colleagues has the credentials to access the desired intellectual property. The accomplices you hire are the targets of the next step. He can force these individuals to assist in the task through financial means, attraction, or physical threats. Then, the insider will succeed to achieve his third goal by accessing restricted data through using the ill-gotten credentials to access the IP. As he desires the exfiltration of a volume of data, the intellectual property will be downloaded to portable media. The final step is covering tracks by deleting the related log files.

This paper has identified how attack-pattern trees are constructed and used to determine the anomaly metric by testing intellectual property theft case studies and stealing clients' money. As mentioned in the research, these two case studies were lake of a unique anomaly identifier for every attack step. This research only addresses how a single employee/actor, its need to address several actors collaborate to accomplish an attack.

This research will use the state transition diagram to model the insider attack steps and the rule-based detection method to detect malicious privilege access.

III. Methodology

3.1 Analysis

[26] showed the concept of attack tree and the constructed attack-pattern tree for intellectual property (IP) theft. The attack pattern used within a machine learning-based threat detection prototype. The attack-pattern tree have defined the attack step and the most prevalent path for each attack type, these attack steps are related to anomaly metrics. The de-constructing of the case studies started by assessing the attack step, then grouping the steps that have a similar meaning. After collecting and modeling enough attacks, the attack steps have been established. Defining the attack steps was the first step to identify attack patterns. attack step in the attack-pattern tree is either can be detected by the machines or required human detection. The tree is also classified into five different classes, as they are normal behavior, covering track, weaponization, attack and outcome

As described in the [26], the steps and the value gained from each step of stealing sensitive IP are described as follows: for gathering intelligence, the insider threat may determine which of their colleagues has the credentials to access the desired intellectual property. The recruiting accomplices are the objective of the next step as he may coerce those individuals possibly via financial means, charm, or physical threats to assist in the task. Then, the insider will succeed to achieve his third goal by accessing restricted data through using the ill-gotten credentials to access the intellectual property (IP). As he desires the exfiltration of a volume of data, the intellectual property will be downloaded to portable media. The final step is covering track by deleting the related log files. In this paper the approach and state transition diagram are novel.

3.2 Methodology

Rule based approach has been used in this model and the path of actors that aims to publish/share sensitive company files to unauthorized parties by individual's insider attack using State Transition Diagram. The diagram well describes the actor steps taken from Normal to Publish state. In addition, the diagram clearly defines the non-suspicious activity that has not reached the Attack state. Suspicious activity means the individuals who are active in normal, weaponize and cover track activities without use attack and publish activities.

According to [28], there are seventy-seven attack steps that can be taken to achieve the goal of publishing sensitive company files by an insider attack. After deep study in attack steps that described in [27] and [28] the consideration is that, some of the attack steps in [27] defined the layers it falls under a designed diagram which is has layered the attack steps based on analysis and aggregated them to five groups. The normal activity group aggregates all normal actions taken by the user. Weaponize group aggregates all action taken to make the item able to damage the target [29]. Covering Track group is an aggregation of all activities attempts to remove the evidence and avoid the detection by the assets' countermeasures [30]. Attack groups aggregate all steps that indicate the illegal activities. The publish group aggregated all steps that the attack conducted to publish or share the intellectual property files. Actor steps will be analyzed offline, which is known according to [31] as the started process is allowed to run for some time, then it is stopped using an external influence. Hence, the offline analysis detection will use the log file after the attack occurred, no matter if it is published.

Activities are grouped as N group consist of Normal activities, W group consist of Weaponize activities, CT group consist of Covering Track activities, A group consists of Attack activities and P group consist of Publishing activities. Activities of each group are defined below:

N [AC2, AC3, AC5, AC6, AC69, and AC75]
W [AC1, AC8, AC9, AC10, AC11, AC12, AC13, AC14, AC15, AC16, AC17, AC26, AC31, AC56, AC59, AC60, AC62, AC63, AC64, AC71]
CT [AC4, AC7, AC18, AC21, AC42, AC43, AC59 AC65, AC66, AC67 AC72, AC73, AC74, AC76 and, AC77]
A [AC19, AC20, AC22, AC23, AC24, AC25, AC27, AC32, AC33, AC34, AC35, AC36, AC37, AC38, AC39, AC40, AC41, AC46, AC47, AC48, AC49, AC50, AC51, AC52, AC53, AC54, AC70]
P [AC28, AC29, AC30, AC44, AC45, AC57, AC58, AC61, AC68]

Some examples of attack path are discovered in [27]. The first path is AC75; AC6; AC11; AC77; AC27; AC58 The actor used his credentials to normally access sensitive company files to which the actor has authorization. When files were accessed, the attack forced the co-workers to access files or systems to assist in the attack unintentionally. The attacker used the company system or assets without authorization or contradict the company policy to cover this track. The attack is executed when downloading files to a portal device, then it's shared to unauthorized parties/websites.

The second path is AC75; AC6; AC27:AC58. The actor used his credentials to normally access sensitive company files for which he has authorization. Then, the files are downloaded to a portal device and shared with unauthorized parties/websites.

The third path is AC75; AC6; AC11; AC27; AC58. The actor used his credentials to normally access

sensitive company files for which he has authorization. When files were accessed, the attack forced the co-workers to access files or systems to assist in the attack unintentionally. The attack is executed when downloading files to a portal device and shared to unauthorized parties/websites.
The fourth path is AC75: AC15:AC76; AC27:AC58. The actor used his credentials to facilitate later attacks by create Backdoors in company systems. The attacker covers this track using remote access or a VPN to access company systems/data from outside the company. Then the attack is executed when downloading the files to a portal device and shared to unauthorized parties/websites.
The fifth path is AC75; AC5; AC27; AC58. The actor used his credentials to make abnormal or unusual access to sensitive company files or information to which he has authorization. Excursion of this attack is achieved when downloading the files to a portal device. The last step is sharing the files with unauthorized parties/websites.
Sixth path is AC75; AC6; AC11; AC27; AC22; AC58. The actor used his credentials to normally access sensitive company files for which he has authorization. When files were accessed, the attack forced the co-workers to access files or systems to assist in the attack unintentionally. The attack is executed when the files are downloaded to a portal device and deleted. The files in the final are shared with unauthorized parties/websites.
The seventh path is AC69; AC7; AC53; AC58. The actor will use the coworker's credentials (to gain access to company systems/data which elevated the privileges). Then, attempt to cover the track by accessing sensitive company files/information to which the actor has no authorization. The attack is accomplished by physical theft of company clients' assets. The files/information in the final is shared with unauthorized parties/websites.
The last path is AC75; AC74; AC7; AC27; AC58. The actor used his credentials. To cover the track, fake or forged credentials used, and sensitive company files/information to which the actor has no authorization has been accessed. execution of this attack achieved when downloading the files to a portal device. The last step is sharing the files with unauthorized parties/websites.
To test the detection efficiency, an example of ten normal paths has been suggested based on the normal activities defined by [26].
The first path is AC75; AC5; AC2. The actor used his credentials to conduct authorized access to sensitive company files or information and conduct abnormal, authorized access to restricted company areas.
The second path is AC69; AC3. The actor will use the coworker's credentials (to gain access to company systems/data which elevated the privileges) and conduct normal, authorized access to restricted company areas.
The third path is AC75; AC6. The actor used his credentials to conduct normal, authorized access to sensitive company files.
The fourth path is AC69; AC5. The actor will use coworker's credentials (typically access company's systems/data which elevated the privileges) to conduct authorized access to sensitive company files or information and abnormally conduct authorized access to restricted company areas.
The fifth path is AC69; AC2; AC5. The actor will use coworker's credentials (to gain access to company systems/data which elevated the privileges) to conduct abnormal, authorized access to restricted company areas and sensitive company files or information.
The sixth path is AC75; AC3. The actor used his credentials for normal and authorized access to restricted company areas.
The seventh path is AC75; AC2. The actor used his credentials to conduct abnormal, authorized access to restricted company areas.
Eighth paths is AC69; AC6. The actor will use the coworker's credentials (to gain access to company systems/data which elevated the privileges) to conduct normal, authorized access to sensitive company files.
Ninth path is AC69; AC5; AC2. The actor will use coworker's credentials (to gain access to company systems/data which elevated the privileges) to conduct authorized access to sensitive company files or information and conduct abnormal, authorized access to restricted company areas.
Tenth path is: AC75; AC6; AC3. The actor used his credentials to conduct normal, authorized access to sensitive company files and access to restricted company areas.

3.3 Assumptions

1- Based on [27], The last classification layer in the attack tree is the outcome layer However, the deep analysis of paths deduces an assumption that the attack intention existed at the attack layer. Hence, the attack state is an announcement that the system is compromised.
2- Based on the first assumption, even if the actor did a normal, weaponized, or covering track activities after attack activity, the system remains in an attack state and still compromised.
3- Regardless of the attack outcome which is referred to in the diagram as publish state. The main concern of our method is the attack state.
4- The attacked state is only achieved after the system gets into an attack state.
5- The repeated action from a specific group

won't change the state.

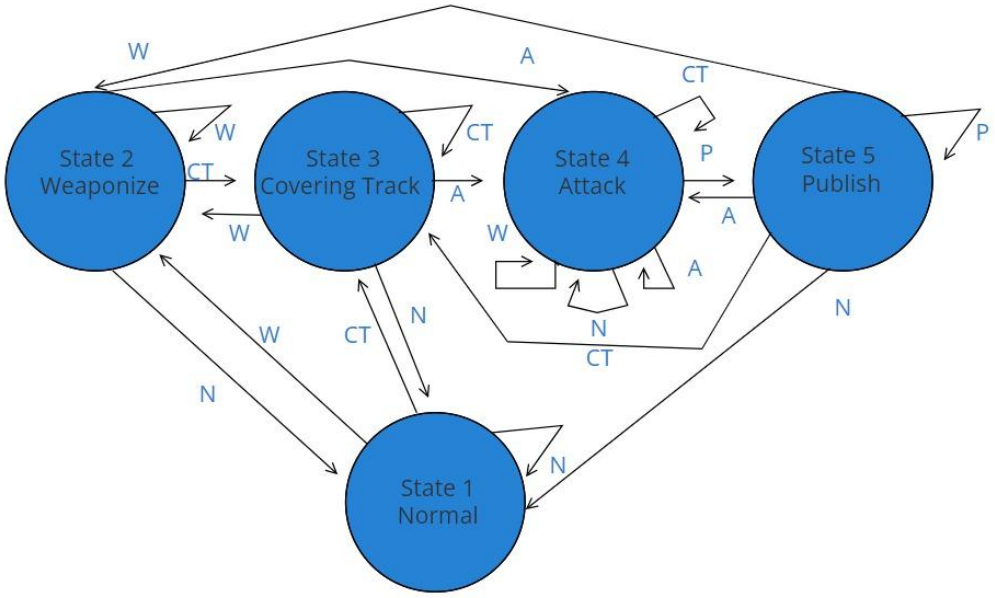

Figure 1 State Transition Diagram

The model starts at a normal state, and the arcs represent transferring from one state to another state based on the action taken.

- Group N can transfer the state from weaponized state to normal state, from cover track state to normal state or from publish state to normal state.
- Group W can transfer the normal state to the weaponize state, the covering track state to weaponize state, from the weaponize state to attack state, or from the publish state to the weaponize state.
- Group CT can transfer the normal state to the cover track state, from the weaponize state to the cover track, or from the publish state to the cover track state.
- Group A can transfer the weaponize state or cover track state to attack state and from publish state to attack state.
- Group P can transfer the attack state to the publish state.

3.1 State Transition Diagram

According to [22], the state transition diagram is a graphical representation of a penetration scenario, and it is constructed of nodes that represent the states, and arcs that represent the actions. Based on the assumptions, the state diagram constructed as below:

3.2 Rules

Based on the state transition diagram the rules are stated and used for detecting the insider attack are sixteen if-then rule.

1. IF state is normal and CurrentActivity is W THEN state is Weaponize.
2. IF state is normal and CurrentActivity is CT THEN state is Covering Track.
3. IF state is Weaponize and CurrentActivity CT THEN state is Covering Track.
4. IF state is Weaponize and CurrentActivity N THEN state is normal.
5. IF state is Weaponize and CurrentActivity A THEN state is Attack.
6. IF state is Covering Track and CurrentActivity is A THEN state is Attack.
7. IF state is Covering Track and CurrentActivity is W THEN state is Weaponized.
8. IF state is Covering Track and CurrentActivity is N THEN state is normal.
9. IF state is Attack and CurrentActivity is P THEN state is Publish.
10. IF state is Attack and CurrentActivity is N THEN state is Attack.
11. IF state is Attack and CurrentActivity is W THEN state is Attack.
12. IF state is Attack and CurrentActivity is CT THEN state is Attack.
13. IF state is Publish and CurrentActivity is A THEN state is Attack.
14. IF state is Publish and CurrentActivity is N THEN state is Normal.
15. IF state is Publish and CurrentActivity is W THEN state is Weaponize.
16. IF state is Publish and CurrentActivity is CT THEN state is Cover Track.

3.3 Pseudocode

Pseudocode is a java language pseudocode which stated based on rules and state transition diagram. Three classed are initiated, State class, Current Activity class, and the insider detection class. State and current activity class are called in the insider detection class.

```
Class State
String = "Normal"
String = "Weaponize"
String = "Cover Track”
String = "Attack"
String = "Publish"
Class CurrentActivity
String = “N”
String =  “W”
String = “CT”
String = “A”
String = “P”
Class UserId
Useride = “01”
Useride = “02”
Useride = “03”
Useride = “05”
Useride = “06”
Useride = “07”
Useride = “08”
Useride = “09”
Useride = “10”

Class Insider detection
String CurrentActivityVar = CurrentActivity
String States = State
String UserID = Userid
If (States.State = "Normal" & CurrentActivityVar. CurrentActivity = “W”) then
States = "Weaponize"
If (States.State = "Normal" & CurrentActivityVar. CurrentActivity = “CT”) then
States = "Cover Track"
If (States.State = "Weaponize" & CurrentActivityVar. CurrentActivity = “N”) then
States = "Normal"
If (States.State = "Weaponize" & CurrentActivityVar. CurrentActivity = “CT”) then
States = "Cover Track"
If (States.State = "Weaponize" & CurrentActivityVar. CurrentActivity = “A”) then
States = "Attack"
If (States.State = "Cover Track" & CurrentActivityVar. CurrentActivity = “N”) then
States = "Normal"
If (States.State = "Cover Track" & CurrentActivityVar. CurrentActivity = “W”) then
States = "Weaponize"
If (States.State = "Cover Track" & CurrentActivityVar. CurrentActivity = “A”) then
States = "Attack"
If (States.State = "Attack" & CurrentActivityVar. CurrentActivity = “P”) then
States = "Publish"
If (States.State = "Attack" & CurrentActivityVar. CurrentActivity = “N”) then
States = "Attack"
If (States.State = "Attack" & CurrentActivityVar. CurrentActivity = “W”) then
States = "Attack"
If (States.State = "Attack" & CurrentActivityVar. CurrentActivity = “CT”) then
States = "Attack"
If (States.State = "Publish" & CurrentActivityVar. CurrentActivity = “N”) then
States = "Normal"
If (States.State = "Publish" & CurrentActivityVar. CurrentActivity = “W”) then
States = "Weaponize"
If (States.State = "Publish" & CurrentActivityVar. CurrentActivity = “CT”) then
States = "Cover Track"
If (States.State = "Publish" & CurrentActivityVar. CurrentActivity = “A”) then
States = "Attack"
```

3.4 Data Structure

Log file generated to be used as an input to the designed Rule-based detection method consists of the user’s activity as User ID. The time and date of conducting an activity on the system. The activity code is from AC1 to AC77.

Acknowledgments
The completion of this undertaking could not have been possible without the participation and assistance of so many people whose names may not all be enumerated. Their contribution is sincerely and gratefully acknowledged.
However, the group would like to express their deep appreciation and indebtedness particularly to the following:
Dr. Manar Salamh and Dr. Salma Kammon
To all relatives, family, friends and others who in way or in another share their support, thank you.
We thank you.

Bibliography

[1] Probst, C. W. (2010). Insider threats in cyber security. Springer.
[2] Three categories of security controls. LBMC Family of Companies. (2020, December 2). Retrieved December 18, 2021, from https://www.lbmc.com/blog/three-categories-of-security-controls/
[3] Initiative, J. T. F. T. (2011, March 1). Managing information security risk: Organization, Mission, and information system view. CSRC. Retrieved December 18, 2021, from https://csrc.nist.gov/publications/detail/sp/800-39/final
[4] Freund, J., & Jones, J. (2015). Measuring and managing information risk a fair approach. Elsevier, Butterworth-Heinemann.
[5] Payne, J. (2020). Inside jobs: Why insider risk is the biggest cyber threat you can't ignore. Skyhorse Publishing.
[6] Bupa fined £175,000 for systemic data protection failures. ICO. (n.d.). Retrieved December 18, 2021, from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/bupa-fined-175- 000-for-systemic-data-protection-failures/
[7] 5 real-life examples of breaches caused by insider threats. 5 Real-Life Examples of Insider ThreatCaused Breaches | Ekran System. (2021, November 25). Retrieved December 18, 2021, from https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches
[8] Standardization, I. O. for. (n.d.). Iso/Iec 27001:2013: Information Technology -- security techniques -- information security management systems -- requirements. International Organization for Standardization.
[9] Force, J. T. (2020, December 10). Security and Privacy Controls for Information Systems and organizations. CSRC. Retrieved December 18, 2021, from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[10] Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E., & Ducheneaut, N. (2012). Proactive insider threat detection through graph learning and psychological context. 2012 IEEE Symposium on Security and Privacy Workshops. https://doi.org/10.1109/spw.2012.29
[11] Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. Procedia Computer Science, 45, 436–445. https://doi.org/10.1016/j.procs.2015.03.175
[12] Data Analytics for Insider Threat Detection. MILCOM 2015 - 2015 IEEE Military Communications Conference. https://doi.org/10.1109/milcom.2015.7357562
[13] Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2017). Automated Insider Threat Detection System Using User and Role-Based Profile Assessment. IEEE Systems Journal, 11(2), 503–512.
[14] Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J., & Fang, B. (2018). Insider threat detection with deep neural network. Lecture Notes in Computer Science, 43–54. https://doi.org/10.1007/978-3-319-93698-7_4
[15] Le, D. C., Zincir-Heywood, N., & Heywood, M. I. (2020). Analyzing data granularity levels for insider threat detection using machine learning. IEEE Transactions on Network and Service Management, 17(1), 30–44. https://doi.org/10.1109/tnsm.2020.2967721
[16] Anomaly detection for insider threats using unsupervised ensembles. IEEE Xplore. (n.d.). Retrieved December 17, 2021, from https://ieeexplore.ieee.org/document/9399116
[17] Kent, K., & Souppaya, M. P. (2006). Guide to computer security log management. https://doi.org/10.6028/nist.sp.800-92
[18] IBM. (2021). IBM: 2021 X-Force Threat Intelligence index. Network Security, 2021(3), 4–4. https://doi.org/10.1016/s1353-4858(21)00026-x
[19] Bitglass. (2019). Bitglass 2019 Insider threat report: 41 percent of organizations do not monitor user behavior across their cloud footprints. Bitglass. Retrieved December 18, 2021, from https://www.bitglass.com/press-releases/threatbusters-2019-insider-threat-report
[20] Liu, L., de Vel, O., Han, Q. L., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Communications Surveys & Tutorials, 20(2), 1397–1417.

https://doi.org/10.1109/comst.2018.2800740
[21] Salem, Malek Ben, et al. "A Survey of Insider Attack Detection Research." Insider Attack and Cyber Security, 2008, pp. 69–90, 10.1007/978-0-387-77322-3_5.
[22] Ilgun, K. (1993). USTAT: a real-time intrusion detection system for UNIX. Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy. https://doi.org/10.1109/risp.1993.287646
[23] Berlin, Konstantin, et al. "Malicious Behavior Detection Using Windows Audit Logs." Www.arxiv-Vanity.com, 13 June 2015, www.arxiv-vanity.com/papers/1506.04200/. Accessed 27 Feb. 2022.
[24] Cinque, Marcello, et al. "Event Logs for the Analysis of Software Failures: A Rule-Based Approach." IEEE Transactions on Software Engineering, vol. 39, no. 6, June 2013, pp. 806–821, 10.1109/tse.2012.67. Accessed 17 Dec. 2019.
[25] Farooqi, A. H., Khan, F. A., Wang, J., & Lee, S. (2012). A novel intrusion detection framework for wireless sensor networks. Personal and Ubiquitous Computing, 17(5), 907–919. https://doi.org/10.1007/s00779-012-0529-y
[26] Agrafiotis, I., Legg, P., Goldsmith, M., & Creese, S. (2014, January 1). Towards a User and Role-based Sequential Behavioural Analysis Tool for Insider Threat Detection. ResearchGate. https://www.researchgate.net/publication/275038765_Towards_a_User_and_Role-based_Sequential_Behavioural_Analysis_Tool_for_Insider_Threat_Detection
[27] Agrafiotis, Ioannis, et al. "Identifying Attack Patterns for Insider Threat Detection." Computer Fraud & Security, vol. 2015, no. 7, July 2015, pp. 9–17, 10.1016/s1361-3723(15)30066-x. Accessed 6 May 2019.
[28] RC Nurse, J., Agrafiotis, I., Buckley, O., a Legg, P., Goldsmith, M., & Creese, S. (2015). Insider Threat Attack Steps. Corporate Insider Threat Detection (CITD).
[29] Whitman, M. E., & Mattord, H. J. (2021). Principles of incident response and disaster recovery. Cengage Learning.
[30] Kurtz, J. A., & Kaczmarek, R. (2017). Hacking wireless access points: Cracking, tracking, and signal jacking. Syngress, an imprint of Elsevier.
[31] Lente Gábor. (2015). Deterministic kinetics in chemistry and systems biology the dynamics of Complex Reaction Networks. Springer International Publishing.