International Journal of Advanced Science and Technology
Vol. 29, No. 7s, (2020), pp. 3280-3288

Intrusion Response System based on Time Management Concept with the Critical IP Address as a Parameter

Ariani[1] and Muhammad Salman[2]

[1,2] Faculty of Engineering, University of Indonesia
[1]ariani81@ui.ac.id, [2]muhammad.salman@ui.ac.id

Abstract

The intrusion response system is a component to improve the performance of network security intrusion detection systems (IDS) for choosing the right and optimal response options. An administrator can perform response actions based on the severity of the IDS which is determined by the vulnerability score on CVE based on the CVSS metric base. However, with a large number of intrusions on the internet, an appropriate response is needed by paying attention to the target intrusion to prioritize which intrusion must be resolved. So, we have to determine response options for the most critical assets. The parameters for it are the IP address because the IP address is one of the cores of the internet, which can show the identity of the institution owner the IP.

Keywords: *Intrusion response system, intrusion, severity, critical asset, IP address*

1. Introduction

Internet network technology has developed from various fields such as business, education, government, and social activities within a few years. Along with the development of the substance of these fields threats in network security are increasingly varied. Network security is an issue that has been used as substantial research in the last few years since the late 19th century.

To prevent threats to the network, there are several methods that can be used to survive. Shameli Sendi [1] said that defense life-cycle includes 4 phases, namely: Prevention to prevent threats, Monitoring for monitoring the presence or absence of threats, Detection is detecting threats through the network, and Mitigation, namely reducing threats.

Based on traffic reports in the annual report book published by IDSIRTII-BSSN, the number of intrusions obtained was more than 235 million in 2019 where the number was obtained by using the intrusion detection system (IDS) security mechanism. This indicates that the assessment of internet security in Indonesia has a high-risk status because Indonesia has a high number of open UDP servers and is above the world average. The result is very vulnerable to DDoS attacks through amplifying attacks. If this happens, there will be many services on the internet that die and cannot be accessed by users [2].

There are 3 types of intrusion systems: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Intrusion Response System (IRS). IDS is a system to detect intrusions without taking actions such as a drop action. IPS system is a network security/threat prevention system that checks network traffic flow to detect and prevent exploitation of vulnerabilities.

The weakness of IDS is that it collects from network sources that can detect, analyze and report the occurrence of an intrusion by giving alerts to administrators without responding. Compared between IDS and IPS, one of the most common problems of IPS is the detection of false positives and false negatives, this occurs when the system blocks

activity on an abnormal network so it is assumed to be dangerous, which results in denial of service, valid users, trying to do valid procedures; or in the case of false negatives. IPS requires a system that has high performance and is difficult to manage in analysis and prevents intrusion at the same time. Thus, security measures that continuously monitor system performance are needed to effectively identify and manage potentials called IRS [3].

Based on the defense life cycle phase previously stated, the Prevention phase can use IPS to maintain the system, the Monitoring phase can be carried out using network tools such as SIEM or other self-developed tools. IDS is a detection phase to analyze the presence or absence of a threat. IRS as a mitigation phase of a threat and is responsible for choosing the right response to deal with a malicious anomaly. In the mitigation phase, the selection of appropriate response options is very important in protecting the internet infrastructure so that large adverse impacts can be minimized.

So, in this research, we purpose the response strategy model with critical IP priority to the priorities of the response handled earlier. This purpose to give recommendations and considerations in making decisions about what responses should be made to an intrusion that occurred on the internet network.

Why we use IP address for the priority response, because IP address is a core of the Internet which is unique and different for each other. This IP address also shows the owner of the server on the computer networks.

And why we choose critical sector for first priority because of most of country have critical sector priority to first handle if it had been damaged. We give example in Indonesia. Indonesia also has it. Indonesia have been established the regulation about the sector critical that have electronic data strategic.

This paper will be presented as follows at a glance the defense life cycle phase of the introduction. Section 2 provides related work and previous research. Section 3 consists of a theoretical introduction to the intrusion response system as well as several other theories. Then proceed with section 3 which contains discussions and analysis, and the last is a conclusion.

2. Theory

Along with a large number of assets and intrusions, critical aspects are very important in prioritizing. Research on intrusion response systems is not as much research on intrusion detection systems. If the intrusion detection system research discusses a lot about the choice of methods or algorithms for developing an intrusion detection system, then some previous research on intrusion response systems discusses taxonomy, design, challenges, method models for the response system.

Studies on intrusion response system that have been conducted by several researchers Shameli-Sendi et al (2012 and 2014) Stakhanova et al (2007), Shahid Anwar et al (2017), and Zakira Inayat et al(2015), explains the results of the classification of the Intrusion Response System and emphasizes important aspects related to the Intrusion Response System and security issues. Anuar et al [4] conducted a 4 quadrants model response strategy experiment with case studies on the DARPA 2000 dataset and the Plymouth University dataset. They compared the two Snort priority standards and CVSS v2 to show the mapping process between incidents, priorities and practical needs in the field. 4 quadrants got from the concept of time management, which divided the response types into 4: avoidance, transfer, mitigation, and acceptance. In determining a type of response to an intrusion, Anuar utilizes a 0-10 score of CVSS based CVE by dividing it into 4 threshold ratings that figured in Figure 1.

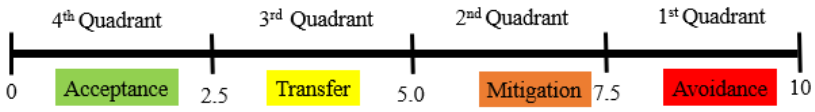

Figure 1. Rating Threshold[4]

2.1. Intrusion Response System

Intrusion Response System is a very important component to improve the performance of network security from intrusion detection systems. IRS is useful for IDS in choosing the right and optimal response options according to the type of network attack [5]. The basic work of IDS is to detect an anomaly or an attack by giving alerts without taking action, so this is where the role of the IRS, namely maximizing IDS performance against anomalies and attempted attacks in real-time with the response that must be done.

In theory, the intrusion response system is divided into several based on taxonomy, including based on the level of automation, response mechanisms, the ability to adjust, response time, cooperation ability, decision-making model selection, response cost, applying location, response lifetime, response selection method[1][5][6].

Intrusion response system based on the level of automation has 3 main types of systems based on the level of automation, namely: notifications, manual and automatic. IRS with a notification system is a response in the form of alerts that contain detected intrusions, both in the form of an attack-type, time of the attack, related IP, etc. which is then used by the administrator to choose what action to take so as not to do prevention directly. The disadvantage lies in the time between notifications that occur with the response made by the administrator who may not always be in real time. In the manual type, the system is more automated because the response to the attack has been configured by the administrator before based on the reported attack information, so the manual type provides a higher level of automation than the notification system. Whereas automatic type systems are designed automatically so that the system performs its own actions without the need to wait for an administrator.

The intrusion response system based on the mechanism is 2 types: passive and active. Passive systems are to inform or provide information about anomalies or attacks. While the active system aims to minimize the impact caused by anomalies or occurred attacks.

Intrusion response system based on time there is 2 types, delay and proactive. Delay response will give notification of response that must be done after an anomaly or attack, while proactive aims to control and prevent anomaly or attack before it occurs. The use of proactive systems is usually used to protect host and network assets from attackers with a possible mechanism, which is now better known as an intelligent threat.

Intrusion response system based on decision-making model selection, there are 2 types, static and dynamic mapping. The static model is easier to define and the process starts with the mapping between incidents and responses manually by the administrator. Anuar said that this decision making strategy can be found in Snort [4], where Snort uses a static notification system to react to anomalies or attacks with decisions that are defined in a simple table. Dynamic mapping it adopts a dynamic decision making and selection approach. The four taxonomies above are intrusion response system taxonomies that are often applied to intrusion detection systems.

2.2. Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is a framework for assessing the characteristics and severity of the impact of a software vulnerability [7]. CVSS is divided

into 3 metrics, where each metric is divided back into several sections, explained in Figure 2.

- Base metrics, which represent intrinsic characteristics of vulnerabilities that are constant and in the user's environment.
- Temporal metrics, which represent vulnerability characteristics that change over time but are outside the user's environment.
- Environments metrics, which represent vulnerability characteristics that are unique to the user's environment.

CVSS is used as a framework in calculating vulnerability for an attack. CVSS calculations are based on metric groups, where each group produces a score of 0 to 10. In addition, there is a Vector String (V) as a text representation of a series of CVSS metrics that are used to transfer CVSS metric information into a summary of values.

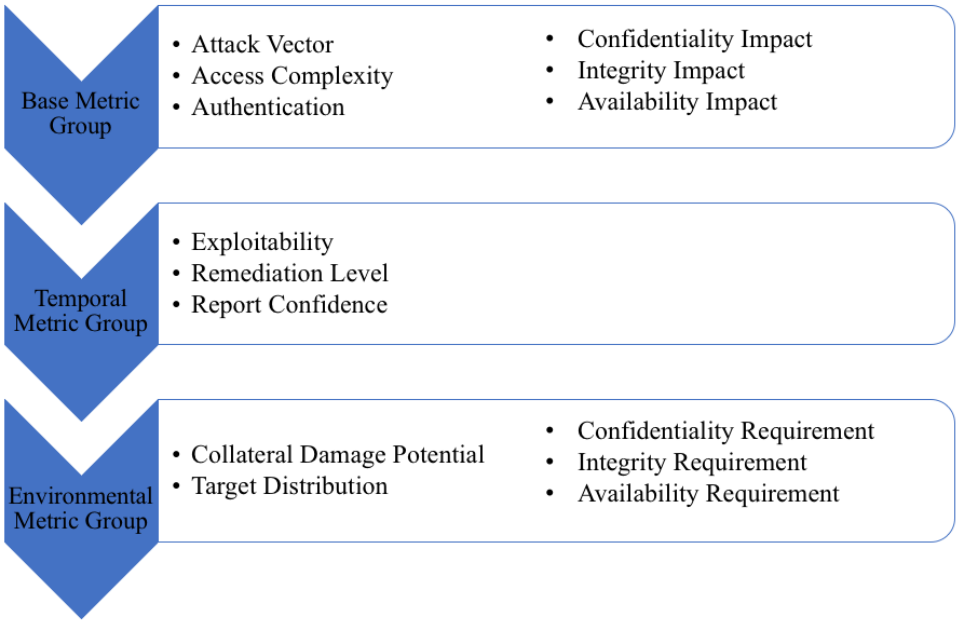

Figure 2. CVSS Metric Group[4]

2.3. Response strategy model with Time Management Concept

Response Strategy Model (RSM) with Time Management Concept is a response model approach that uses a combination of risk response planning and time management concepts to determine a more effective response to anomalies or attacks that occur. This strategy model was carried out by Anuar et al. To create this model for the IRS, Anuar represents the strategy model in 4 quadrants based on an important and urgent time management matrix which is then translated as a form of response when there is an intrusion. The four quadrants translated by Anuar above are Q1 as critical and urgent, Q2 as critical but not urgent, Q3 as not critical but urgent, and Q4 as not critical and not urgent. Following are the 4 quadrants with how the response plan will be given:

a) Q1, critical and urgent: Q1 Q1 has super high priority and must be dealt with immediately because anomalies or attacks or incidents have a large impact or target on critical sectors. The response method provided in Q1 is avoidance so that it does not have an impact on important infrastructure, things that can be done such as blocking.
b) Q2, critical but not urgent: Q2 also has a high priority level, but not too critical. The response used is risk mitigation to minimize the impact caused by attacks and aims to reduce the risk score to a lower risk.

c) Q3, not critical but urgent: Q3 is on the third priority or medium priority, where the conditions are urgent but not critical. The response method used for Q3 is Transfer. This transfer response can be done by adding other tools such as the third party as security to minimize the impact.
d) Q4, not critical and not urgent: Q4 is the lowest priority. This category includes passive responses. This response method is to accept the resulting impact. Usually, this Q4 is only in the form of information and has no impact on assets.

2.3. Internet Governance

Core internet consists of protocols and infrastructure both physically and logic, as well as other supporting infrastructure such as internet infrastructure provider organizations [8] The so-called Internet infrastructure, is DNS, IP numbers, and root servers [9]. Laura DeNardis also mentioned Critical Internet resources (CIRs) such as Internet protocol (IP) addresses, domain names, and autonomous system numbers (ASNs); the Internet's domain name system (DNS); and network-layer systems such as Internet access, Internet exchange points, and Internet security intermediaries[10].

Among these critical internet resources, IP address is the most basic resource needed for information exchange through the Internet, because this unique IP address is useful as the destination and the source address in a communication on the internet, in fact, a physical infrastructure must have an IP address so can be recognized and mutually networked.

In public, different IP addresses can communicate. The system distribution of IP numbers is arranged hierarchically. At the top are IANA (Internet Assigned Numbers Authority which distributes blocks of IP numbers to five regional Internet registries (RIRs). 13 RIRs distribute IPs to local Internet registries (LIRs) and national Internet registries (RIRs), which are then distributed to ISPs, companies, government, to the personal community. The IP is the identity of the owner of the address of an internet network, which defines who the owner is including whether the IP belongs to an institution that has a critical role in national defense.

3. Method

Along with a large number of assets and intrusions, critical aspects are very important in prioritizing asset handling against intrusion. Criticality is defined as an asset that has a high value. Criticality is based on three main and general attributes in security, such as confidentiality, integrity, and availability [11]. So, it can be concluded that the higher the critical level, the greater the impact.

The IP is important as one of the cores of the internet, so IP has a very important role in helping determine priorities in the decision-maker response. So that the severity variable of IP can be an additional parameter in determining decision making to give an intrusion response system effectively as an additional parameter.

3.1. Defining Method Quadrant

Critical IP is defined as a parameter that can change the initial quadrant that was previously only based on the value of the score of CVE. Anuar determines the quadrant response based on the CVE threshold score as shown in Figure 1. By adding a critical IP parameter to the determination of the quadrat response, it can change the previous quadrant.

- If an intrusion is in quadrant 3 (transfer), if the target IP is an IP in a critical sector it will shift to quadrant 1 (avoidance) because the critical axes value shifts from not critical to critical;
- If an intrusion is in quadrant 4 (acceptance), if the target IP is an IP in a critical sector it will shift to quadrant 2 (mitigation), because the value of critical axes shifts from not critical to critical. It also notes that the system has weaknesses, because it is a critical IP and can have an impact on the system;
- However, if the intrusion is in quadrant 4 or 3 with IP that is not in a critical sector, then the quadrant is fixed.

3.1. Critical IP address

IP address data which is an important asset is collected based on the data of critical sector asset owners from the state, this sector has been determined in the existing regulations, as a guideline in national defense. There are 9 sectors [12] that are determined based on regulations, including:

- Government administration sector;
- The energy sector and mineral resources;
- Transportation sector;
- Financial sector;
- The health sector;
- Information and communication technology sector;
- The food sector;
- The defense sector; and
- Other sectors determined by the government.

3. Result and Discussion

This section, experiment aims to investigate the effectiveness of purpose strategy in the intrusion response selection. One of the criteria to support the response selection process is a critical parameter to consider the decision making of the response. Furthermore, this experiment also to analyze the distribution of incident and the critical parameter as one of the important objectives supporting the selection response of the intrusion.

The intrusion event dataset used in this experiment is intrusion data based on snort that has been detected for one month. While IP data is obtained from institutions that have the authority to conduct internet monitoring. Comparative data to calculate the urgency value of an intrusion based on CVE score data in the NVD database. CVE scoring on NVD used is CVSS v2 because the CVE data corresponding to CVSS v2 is more complete than the newer CVSS v3.

The case study of this experiment used with the comparison with other approaches as Snort Priority, CVSS v2 base score, and CVSS v2 base score plus IP as a critical parameter. This experiment used to analyze the differences between the 3 types of them. So, the intrusion response divided into 3 types of responses shown in table 1.

Table 1. Strategy Response

	Snort Priority	**CVSS v2 (base score)**	**CVSS v2 (base score) + IP**
Avoidance	high	>7.51	>7.51 or 2.51-5.0 on IP critical
Mitigation	medium	5.01-7.5	5.01-7.5 or 2.5 on IP critical
Transfer	low	2.51-5.0	2.51-5.0

Acceptance	information	<2.5	<2.5

The explanation of the 3 response strategies as a comparison are:

1) Determination of response based on signature priority divided based on category: high, medium, low, and information.
2) The response based on base score CVSS divided into 4 types of range rating threshold. It means, the scores more than 7.5 must avoid, between range 5-7.5 with mitigation, between 2.5-5 is transfer, while less than 2.5 is accept
3) And the response based on CVSS plus IP parameter divided into 4 types of rating threshold by observing the value of the parameter criticality of the owner of the IP address, so if it is critical then it must shift to quadrat with critical

Table 2 shows the distribution of intrusion in this experiment. It contains 608966 intrusions. The signatures are true incidents. The description of the signature name obtained from the signature snort. The second column in Table I shows the number of intrusions on those signature name.

Table 2. The Experiment Dataset

Signature Name	Total
PUA-OTHER XMRig cryptocurrency mining pool connection attempt	328566
PUA-OTHER Cryptocurrency Miner outbound connection attempt	221244
MALWARE-CNC Win.Trojan.Glupteba C&C server READY command to client	26538
SERVER-WEBAPP PHPUnit PHP remote code execution attempt	11878
MALWARE-CNC Win.Trojan.Zeus variant outbound connection	10236
SERVER-APACHE Apache Struts remote code execution attempt	3804
PUA-OTHER CPUMiner-Multi cryptocurrency mining pool connection attempt	1977
SERVER-WEBAPP Drupal 8 remote code execution attempt	1522
MALWARE-CNC User-Agent known malicious user-agent string - Virut	1336
POLICY-OTHER cryptomining javascript client detected	527
SERVER-ORACLE Oracle WebLogic Server remote command execution attempt	318
MALWARE-CNC Torpig bot sinkhole server DNS lookup	300
PUA-OTHER XMR-Stak cryptocurrency mining pool connection attempt	136
Others	584

Figure 3 shows a different amount of response. When we use selected response based on snort priority, we have to avoid response and must be dealt with the immediately response before have large impact is too high, because attacks up to 99.97% of all total intrusions, and intrusions that must be mitigated are only 0.01% and those that must be transferred are 0.02%.

And when we use rating threshold plus IP as critical parameter, the amount of data response selection in quadrant 1/ avoid and quadrant 2/mitigate increase because of the data intrusion that have to transfer must be mitigated when the target is critical IP.

Selection responses based on the CVSS v2 rating threshold can reduce the number of response responses to intrusion to only 44% handled to avoid attacks. Whereas intrusion that must be mitigated rises compared to snort priority to 56% and that must be transferred rises to as much as 0.47%.

By adding the critical IP parameters, the amount of data response selection in quadrants 1 and 2 increases due to the shift in response to the data in quadrant 3 on the critical IP. Changes to the data are not very significant, but intrusion on the target IP critical must be addressed immediately.

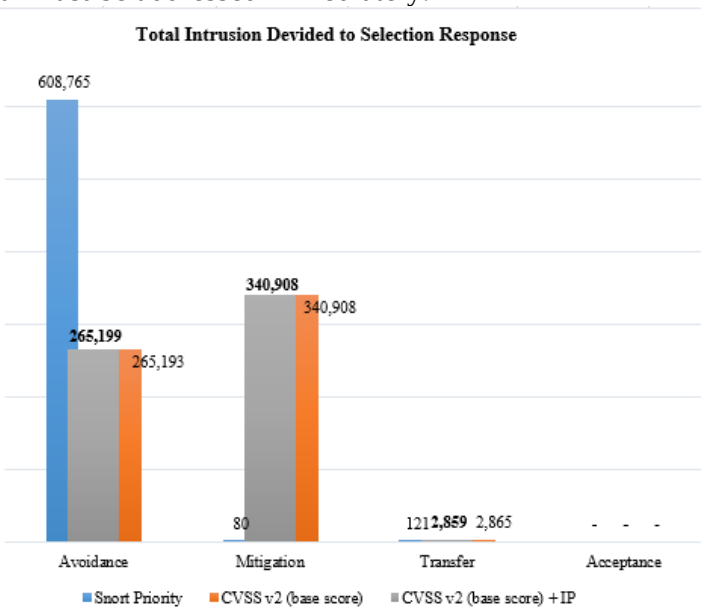

Figure 3. Diagram Total Response Intrusion

By the experiments can be seen that by applying a strategy model with critical IP priority, a responder incident can prioritize which intrusions are handled earlier. So even though the amount of intrusion leading to an IP is large, most IP owners in a critical sector can be handled first to avoid a greater impact.

3. Conclusion

From the experiments can be seen that by applying a strategy model with critical IP priority, a responder incident can prioritize which intrusions are handled earlier. So even though the amount of intrusion leading to an IP is large, most IP owners in a critical sector can be handled first to avoid a greater impact.

In future studies, it may be possible to add criticality values based on assets both physically and data information from the target, so that the determination of quadrants can be more detailed.

References

[1] Shameli-Sendi A, Cheriet M, Hamou-Lhadj A. " Taxonomy of intrusion risk assessment and response system". In Elsevier, 2014.

[2] Indonesia Security Incident Response Team On Internet Infrastructure / Coor Center Annual Report 2018. Available at: idsirtii.or.id

[3] Inayat Z, Gani A, Anuar N, Khan M, Anwar S. "Intrusion response systems: Foundations, design, and challenges". In: Journal of Network and Computer Applications; 2016, vol: 62 pp: 53-74.

[4] Anuar NB, Papadaki M, Furnell S, Clarke N. "A response selection model for intrusion response systems: Response Strategy Model (RSM)". In: Security Comm. Networks, 2014 7:1831–1848; 2013.

[5] Anwar S, Zain J, Zolkipli M, Inayat Z, Khan S, Anthony B, Chang V. "From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions". Publisher: MDPI s, 2017

[6] Stakhanova N, Basu S, Wong J. "A taxonomy of intrusion response systems". Int. J. Information and Computer Security, Vol. 1, No. 1/2, 2007

[7] Common Vulnerability Scoring System version 3.1. available at: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

[8] Osho O., Ojeniyi J.A, Abdulhamid S.M. “Protecting the Core (of the Internet)”, Briefings From The Research Advisory Group, New Delhi 2017

[9] Kurbalija J. “An Introduction To Internet Governance 6th Edition”, 2014

[10] DeNardis L. “Hidden Levers Of Internet Control”, Information, Communication & Society, 15:5, 720-738. 2012

[11] Jumaat, Anuar N.B. “Incident Prioritisation for Intrusion Response Systems”. 2012. 04 University of Plymouth Research Theses.

[12] “Peraturan Pemerintah Indonesia Nomor 71 Tahun 2019 Tanggal 10 Oktober 2019”. Article 99 paragraph 2.