A Virtual & Pragmatic Analysis on Networked Security Incident, its Handling & Reporting Measures

Gyana Ranjana Panigrahi, Nalin Kanta Barpanda and Madhumita Panda

January 5, 2020

A Virtual & Pragmatic Analysis on Networked Security Incident, its Handling & Reporting Measures

Gyana Ranjana Panigrahi[1], Dr Nalin Kanta Barpanda[1], Dr Madhumita Panda[2]
[1]Department of Electronics, Sambalpur University, Burla, India
[2]Department of Computer Science Engineering, Sambalpur University, Burla, India
emails: gyana.ranjana.panigrahi@suiit.ac.in, nkbarpanda@suiit.ac.in, mpanda@suiit.ac.in

Inevitably, it requires an immediate upgrade, update & deployment in the form of reporting of resources and establishment strategies. Today's digital era offers a golden moment to hackers where many a beset corporation facing tough situations by giving much money & time, to breach the valuable data for others. Different actors' and their actions can raise different possibilities of damage like potential risk insiders having the own set of nasty intentions, some insiders are trusted but can cause severe impairment by blunder, and actors like cybercriminals by nature of attacks. Associates and corporations have to take some other form of practical steps whereby responding to the occurred events and their time of incidents appropriately. For reduced performed incidents and responses, there may be a significant chance of affecting the organization primarily for the sector like SOHOs or MNCs significantly in the form of monetary losses, tarnishing of status and perhaps even drive it out of business altogether.

Keywords: Networked Security, CIA Triad, Availability, Potential Threat, Incident Response & Reporting formats.

1. Introduction

Linearly & apparently, it may say that over the time for the past few years the potential IT system can neither qualify nor quantify how harmful its attacks, impacts and compensations have been to the current digital society, is entirely unexpected. Over and above, to meet the need of different requirements of SOHOs (Small Office Home Office), MNCs (Multi-National Companies) and their infrastructures, it is very much difficult to evaluate the impact of risk using traditional isolated tools for guarding against today's risk landscape for protection of sensitive data [1][2]. In return, it leads to a root of incomplete information. Therefore, there might be a chance of enhancing the existing condition by overall risk findings which helps to bridge the problems in between the sufferers and establishments in a distinct manner [3][4][5]. Therefore, over time different supportive methods could be adopted for strengthening the overall process by handling and recovering the data from severe conditions for the basis of the substantial information-sharing scheme [6][7]. Recognition of security cracks is, therefore, highly necessary to aware of the association when incidents materialize. These findings, therefore, improve the way of threat detection and their moderation of traditional as well as upcoming updated bouts by the help of skilled experts and individual participants [8][9]. Therefore, there may be an insight into presuming the exchange of threat and their corresponding technologies can substantially develop a critical cyber threat defense model and its allied technologies within companies [10]. Here in threat intelligence, the pre-defined data and their formats can utilize for sharing the techniques within and out of the infrastructures [11]. Moreover, indirectly the used data format describes the density of respective information. Electronic format exchanging and handling out about threats and incidents of information has widely expected in the area of data exchange [12][13]. Looking at the nature of incident severity, the company can alleviate the effect of the incident by containing and getting better from it [14].

2. Literature Review

With good vision and by dint of onerous effort, many a researcher managed to propound their valuable systematized investigations scientifically with the aid of standard Formats, tools and simulators, out of which below are some of findings relative to current area of work where it can be bridge between security incident, its handling and reporting issues and their respective measures chronologically. As by Karabacak, B., & Sogukpinar, I. (2005) group of scholars, they have focused and offered a deliberate resolution taking the assistance from the area of information security, risk analysis, quantitative risk analysis, paper-based risk analysis & risk model. Where it has been merely concentrated upon an original method on data safekeeping menace investigation system "ISRAM" which is an anticipated quantifiable approach towards the networked security measures. As by Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009) group of researchers, they have engrossed and presented a thoughtful solution by taking the backing from the area of network security. From a different source of threats, intrusion detection anomaly detection, IDS community & assessment has emphasized in the field of NIDS, which is the only source of the mechanism by offering its behavioural profiles through classification. As by Kartaltepe, E. J., Morales, J. A., Xu, S., & Sandhu, R. (2017, June) group of scholars, what they have wanted to suggest is that the current generation of social network-based botnet command & control (C&C), we envision the growth of C&C methods and explore social networks-based countermeasures. As by Choo, K. K. R. (2011) researcher, what he has decided to present is the scheme about different risks by plummeting the opportunities for networked crime through networked felonies to render and commit by augmenting the intensities of different risks whereby. Inferring the submission by backing from the area of Culture of security, networked crime, networked exploitation, policing and preventative strategy, Public, private partnership & routine Activity Theory. As by Liao, H. J., Lin, C. H. R., Lin, Y. C. & Tung, K. Y. (2013) group of researchers who have offered a scheme that the amount of intrusions has excessively increased year by year. Using the CIA triad and their policies testing through VM machines, it is a bit easy to simulate the entirety to leverage the use of disaster from its legacy. However, different techniques may result in the problem of hard creating and updating the knowledge for given attacks. As by Genge, B., Kiss, I., & Haller, P. (2015) group of scholars who have developed and suggested a novel methodology for assessing the impacts of networked-attacks on critical infrastructures. Metrics have proposed for quantifying the significance of control variables and measuring the impact propagation of networked-attacks by backing the aid from the area of Critical Infrastructures, Networked Attacks, Impact Assessment, System Dynamics, Sensitivity Analysis & Smart Grid. As per Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018) group of scholars who have suggested by taking the assistance from the area of networked security assessment, computer personnel selection, training and leadership, sociometric, social sensing, wearables technology, team processes, team development & collaboration and submitted by inferring through different ongoing networked-attacks.

3. Containment, Eradication and Recovery

Organizations must determine acceptable risks in managing the event before and after using various incident procedure mechanisms, and strategies must be developed accordingly. The previous and subsequent steps should focus on long-term changes (for example, infrastructure changes) and on-going tasks to keep the business as secure as possible since disposal and recovery actions are usually specific to the operating system or application.

3.1. Vulnerability in virtualization (Virtual machines):

It is indeed essential to examine the real executions due to the absence of all current infrastructures and their sets, which is only possible by one application, i.e. virtual machine (VM) using the software VMware to emulate real machine functionality. Figure 1 is an overview of VM architecture which shows the way of isolating virtual networks, its accountabilities and bout effects in private to the public network. Still, there is a chance of revealing new-fangled safekeeping exposures using VMware. For example, it is an estimation for DDOS that of about 60 & 30 per cent of virtual machine's results and distributions are less secure than their original corresponding part. Looking at this, we have to maintain the ratio rate of security keepings & its vulnerabilities in that fashion to endure the gap between real to the virtual by the time real-time implementation.

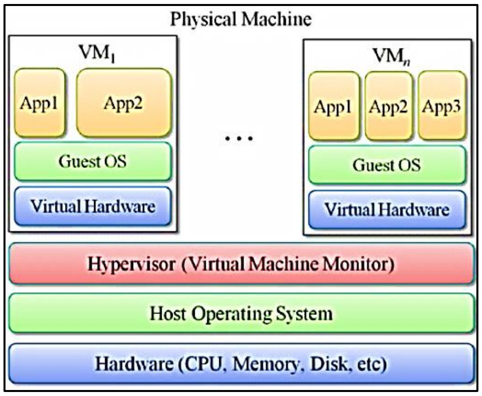

Figure 1 is an overview of VM architecture

4. Hypothesis Design

Having a great experience to solve the related issues, we have to create a stable design for mitigating the gap between different incident scenarios to meet the need of different incident management stakeholders. Where we have to work upon four necessary arms of this design to follow. Motivation to work on this is due to a million different things can go wrong with a computer network on any given day from a simple spyware infection to a complex router configuration error, and it's impossible to solve every problem immediately. It should take a multidisciplinary approach to help & ensure that their clients' sensitive payments, financial and personal information remains private and safe. The scope of the present work, i.e. "A Virtual & Pragmatic Analysis on Networked Security Incident, its Handling & Reporting Measures" is meant to be a study of combination. Many invasion finding techniques, methods and algorithms help to detect these attacks. The objective is to study and compare the consistency of different system and network admin tools on a common platform between traditional and modern methodologies under similar assumptions. The study has required modification of a few existing techniques and development of some new ones, in a manner suitable to obtain the required results in a more straightforward and computationally more efficient manner at hand to be work with a different organization.

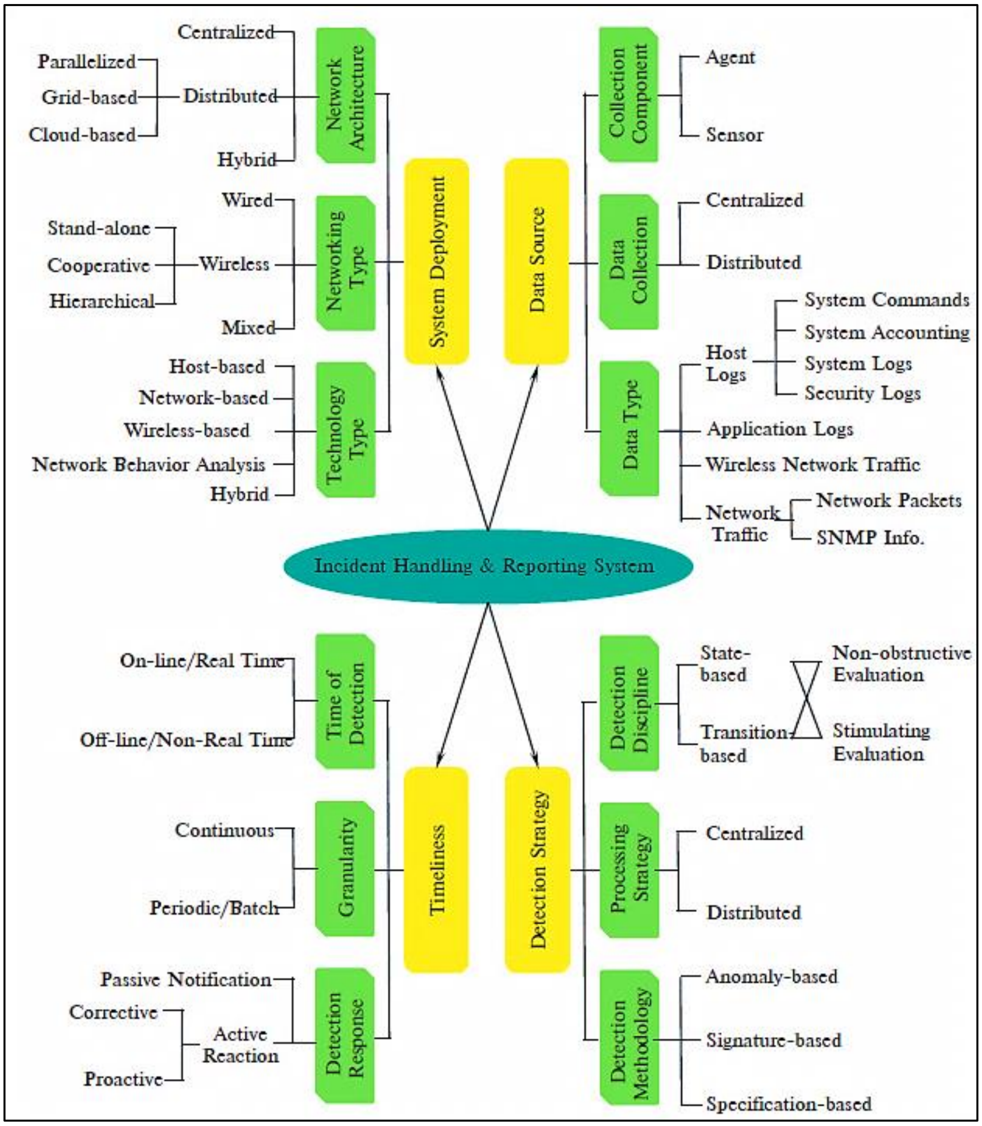

Figure 2 Hypothesis Design.

Incident management methodologies have classified as three major categories: Signature-based Detection (SD), Anomaly-based Detection (AD) and Host-state based description (DS). Table 1 displays table of for and against three finding methods using its types & parameters. Table 2 displays technical summarization of most common traditional tools.

Table 1 shows for and against of invasion finding methodologies:

For and against of invasion finding methodologies.			
	Signature-based (knowledge-based) (SD)	Anomaly-based (behaviour-based) (AD)	Host and State Table Analysis (Based on the description) (DS)
For (Arguments)	• Modest and operative for detection of recognized bouts.	• Real and unknown exposures. • Less reliant on OS.	• Distinguished protocol states.

	• Feature background investigation.	• Enable findings for pleasure misuse.	• Differentiate unpredicted orders for instructions.
Against (Considerations)	• Not so effective identified and unidentified bouts. • Less distinct about protocols. • Updating is a bit difficult. • It takes much time to understand its data.	• Weak & dynamic property. • Inaccessible through behavioural profiles up-gradation. • Hard to activate warnings on immediate demands.	• Resource incontrollable. • Incapable of examining bouts. • Unsuited different apps and OSs.

Table 2 technical summarization of most common traditional tools:

Tool Name	Community	TCP Layer	Area/Technique	Category Unique Identifier	Hybrid	Response	Anomaly related techniques
Nmap	D/ND	L3	Information security awareness & enforcement.	Identify & Detect		Y	Context-aware detection, correlation and multi-dimensional detection engines
OpenVAS	D	L2, L3	Ethical Hacking & Countermeasures.	Identify & Detect	Y	Y	Protocol analysis, pattern matching Behavior-based analysis, statistical analysis, correlation
OSSEC	D	L2	Ethical Hacking & Countermeasures.	Identify & Detect	Y		Application-level semantics, event analysis

Security Onion	D	L2, L3	Information security awareness & enforcement.	Identify, Detect & Respond	Y		pattern matching, protocol analysis Confidence indexing
Metasploit Framework	D/ND	L1, L2, L3	Information security awareness & enforcement.	Identify, Detect & Respond	Y	Y	Behaviour analysis, statistical analysis

Note: The ‘‘Hybrid’’ is the hybrid detection, and the ‘‘Response’’ means some kind of response mechanism is also available. D is related to the DOS platform and ND related to Non-DOS platform.

Conclusion

Firewalls, anti-virus, and IDS have their place in the security landscape, each with its unique features. However, our scheme is that proactive capabilities may help to keep our networks safer from more sophisticated attacks. Before purchasing a product, study the detection and prevention mechanisms, vendors have implemented vis-a-vis current attack methods. An IT asset is any company-owned information, system or hardware that has used in the course of business activities. Hence by preferring a proper research design methodology, any attack and their sophistication can be avoided to present the best scheme of solution at hand.

References:

1. Kritzinger, E., & von Solms, S. H. (2010). Networked security for home users: A new way of protection through awareness enforcement. Computers & Security, 29(8), 840-847.
2. C. Blackwell, A Security Ontology for Incident Analysis, In CSIIRW '10 Proceedings of the Sixth Annual Workshop on Networked Security and Information Intelligence Research, 2010, doi:10.1145/1852666.1852717.
3. ENISA, Good practice guide for incident management, 2010, pp. 60, https://www.enisa.europa.eu/publications/good-practice-guide-for-incident management/at download/full Report.
4. Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., & Williams, T. (2011). Grey hat hacking the ethical hacker's handbook. McGraw-Hill Osborne Media.
5. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
6. O. Deniz, H.B. Celikoglu, Overview to some existing incident detection algorithms: a comparative evaluation, In: Procedia Social and Behavioral Sciences, 02011, pp. 1–13.
7. Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation computer systems, 28(6), 833-851.
8. P. Cichonski, T. Millar, T. Grance, K. Scarfone, Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, In NIST Special Publication Volume: 800-61 Revision 2, 2012, pp. 79, doi:10.6028/NIST.SP.800-61r2.

9. Chonka, A., Xiang, Y., Zhou, W., & Bonti, A. (2011). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, 34(4), 1097-1107.Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for networked security risk planning. Decision Support Systems, 51(3), 493-505.
10. Choo, K. K. R. (2011). The networked threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.
11. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
12. MITRE Corporation, Making Security Measurable, In Proceedings - IEEE Military Communications Conference MILCOM, 2011, pp. 1–9, ISBN: 9781424426775.
13. J. Kohlrausch, S. Übelacker, G. Jra, T. Internal, X-ARF: A Reporting and Exchange Format for the Data Exchange of Netflow and Honeypot Data, 2011, http://geant3.archive.geant.net/Media_Centre/Media_Library/MediaLibrary/xarf_geant_milestone2.pdf.
14. P. Cichonski, T. Millar, T. Grance, K. Scarfone, Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, In NIST Special Publication Volume: 800-61 Revision 2, 2012, pp. 79, doi:10.6028/NIST.SP.800-61r2.
15. Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. Computers & Security, 24(2), 147-159.
16. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security, 28(1-2), 18-28.
17. Alqatawna, J. F., Madain, A., Ala'M, A. Z., & Al-Sayyed, R. (2017). Online social networks security: Threats, attacks, and future directions. In Social Media Shaping e-Publishing and Academia (pp. 121-132). Springer, Cham.
18. Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.
19. Liao, H. J., Lin, C. H. R., Lin, Y. C. & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.
20. Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, 10, 3-17.
21. Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018). Sociometrics and observational assessment of teaming and leadership in a cybersecurity defense competition. computers & security, 73, 114-136.