iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** XI **Month of publication:** November 2020

DOI: https://doi.org/10.22214/ijraset.2020.32263

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XI Nov 2020- Available at www.ijraset.com

Mobile Network Security using Honeypot

Rashmi Shravan Dhanawade
Research Student Department of Information Technology, B. K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan

Abstract: Nowadays smartphone, tablets, PC such devices are widely used i.e. Almost everyone is using such types of devices and they are attractive target for cyber criminal. The main aim of NEMESYS approach is not only research and development of novel security Technology for identification and prediction of abnormal activities which are observed on Smart mobile network but also for gathering and analysing information about method of cyber attack. Mobile honeypot is filled with vulnerabilities and it can be help to generate real idea about the attack methods that can be shared with other users or system security to prevent against them. Online survey was taken to attain proposed hypothesis. With the help of quantitative analysis proposed hypothesis is accepted.

Keywords: Mobile network security, Honeypot, Types of honeypot, NEMESYS approach, Threshold mechanism.

I. INTRODUCTION

Mobile phones makes life more easier. With one device you can make calls, take pictures, send messages, use GPS and many more things. The primary goal of computer security is to defend computers against attacks done by malicious users. Honeypots are designed to be attack targets, mainly to learn about cyber-attacks and attacker behaviours. Honeypot can help to generate real statistics about the attack methods or behaviour of attacker that can be shared with other users or system security to prevent it. When honeypots are implemented within security posture, it also protect real networks by acting as a decoy, deliberately confusing potential attackers as to the real data. Due to the increasing level of malicious activity seen on today's Internet, organizations are beginning to deploy mechanisms for detecting and responding to new attacks or suspicious activity, called Intrusion Prevention Systems (IPS)[18].The two main mechanisms are honeypots and anomaly detection systems [3][4]. Anomaly detection system detects exactly which type of attack is done on the system . Honeypots and anomaly detection systems offer different trade-offs between accuracy and scope of attacks that can be detected . Honeypots can be heavily instrumented to accurately detect attacks, but be determined by an attacker attempting to exploit a vulnerability against them. Also the Threshold mechanism [7] effective in identifying attackers IP address. There are two types of honeypots first is research honeypot used in other one is the production honeypot. Detailed design of a mobile honeypot is introduced in this paper also the implementation of NEMESYS [5][1]. Best honeypot design requires daunting, and skills that make Honeypot design a challenge for the most experienced software architects. Shadow honeypot [8] combines the best features of honeypots and anomaly detection.

A. Types of Honeypot

The author Lance Spitzner define honeypot as, A honeypot is security resource whose value lies is being probed, attacked or compromised. Basically honeypot is filled with full of vulnerabilities when attackers attacks on that vulnerability attacker trapped. This concept is same as pot is filled with honey. In 1998 first honeypot was introduced . The resource was documenting in form of book by Clifford Stoll titled 'The cuckoo's egg' [19][20].There are two types of honeypots [6][19] .

1) *Research Honeypot:* Research honeypots are designed to find out information about attackers such as attackers IP addresses and software or tool which used to harm .The primary aim of research honeypots is to find question like what type of attack is done, By whom attack is done.
2) *Production Honeypot:* Commercial organizations uses production honeypots to detect the attacks against any loss. It is difficult to break or harm to production honeypots.

Further more honeypots are classified between the levels of interactions[6][19].
Low-interaction honeypots are easy to install and configure , deploy and maintain and level of risk is low in Low-interaction honeypots.
Medium-interaction honeypots are involved to install and configure, deploy and maintain and level of risk is medium here.
High-interaction honeypots are difficult to install and configure, deploy and maintain and level of risk is high in High-interaction honeypots.

©IJRASET: All Rights are Reserved

II. OBJECTIVES

To know population really wants to protect their personal or organizational information against any malicious activities.
This objective can attain by examine through survey analysis. Hence we present hypothesis as-

1) *Hypothesis*- When attacker attacks on mobile network (public) then we can detect information about malicious activities using honeypot.

III. LITERATURE REVIEW

[1]Identification and prediction on of abnormal activities which were observed on smart mobile network through NEMESYS approach of mobile honeypot said the author Gelenbe et al. The author Ahmed et al [2] explained about how Android OS choose to analyse the data using static and dynamic techniques as it was extremely high ratio of malware targeting it .The author Gelenbe et al [3] This article was about the analysis the network traffic and development of anomaly detection. Also malware algorithms by combining modelling and learning using network measurement. Used of OPENET was also discussed . [4]The author Gelende et al introduced how DCI help in definition on approach of input representing normal and malicious network activities. Also explained about mechanism of virtualized mobile honeypot and anomaly detection. In [5] article the author Kleber et al presented a novel method to infer structure from network message of binary protocols and implementation of NEMESYS approach. Also introduced two major contribution of network message.
In this article [6] the author Ahmed Salman et al explained how honeypot protected real networks by acting as a decoy and honeypots were used to describe the dark network address space. Also said building an accepted mobile honeypot was a big challenge because of the limited sources and complexity of program required to achieve honeypot function. In article [7] the author Krishnamurthy explained overall about threshold mechanism and how threshold mechanism effective in identifying IP address and BGP protocol used in Mohonk implementation. The author Anagostakisy [8] introduced the architecture and implementation of shadow honeypot.
And also explained how IDS was used to detect suspicious activities. Loosely coupled shadow honeypot was limited to protecting against static attack. In article [9] the author Mokulbe et al described different types of honeypot and an overview of honeypot concept and approaches. In future honeypot could be used to collect information about attackers and other threats they could be useful tool in digital forensics investigation. The author Zhug et al [10] presented an integrated toolkit called honey bow. Which is able to collect autonomous spreading malware in an automated manner using high interaction honeypot. [11] This article was about an overview of the design and implementation of honeyed. For creating virtual honeypot. Also the author Proxos explained how honeyed supports TCP, UDP and ICMP. The author Yehneswaran et al [12] explored methods to integrate honeypot data into daily network security monitoring with goal of sufficiently classify and summarizing the data. Still the author expressed a restriction that they haven't yet attain an integrated analysis that accurately classified events. The author J et al [13] article introduced new approach Outlier detection which helps to find anomalies more effectively than others. The article[14] the author Kreibich et al explained how system applied pattern matching techniques and protocol packet header conformance test on traffic captured on honeypot. [15] The author Song et al performed various experiments to find out and analyse performance of the unsupervised anomaly detection techniques with the help of traffic data.

IV. METHODOLOGY

The proposed research problem is to detect the malicious activities using honeypot since quantitative data is used to achieve that aim. Primary data is collected for the data collection. In this paper sampling method was used for an online survey form. .The survey form was created using Google form. The survey link was circulated in social media platform. The questionnaire in the survey form were designed in such way to test the proposed objective . The survey was collected from Thane district of India. There were 34 people's take part in survey. Among that 52.9% were male and 47.1% were females. Chi-square test was applied to analyse the quantitative data because it is suitable method to attain the proposed objectives.

V. EXPERIMENT

Chi-square test is used to analyse the data in statistical way. The outcome of the test got X^2 calculated as 11.3129 and x^2 tabulated as 3.841 at significance level 0.05.Since x^2 tabulated <X^2 calculated here, the null hypothesis is rejected i.e. People don't want to spend money for protecting their personal or organizational information is rejected.
By this scenario (as shown in Fig 1) it is accepted that the people's are more conscious about their personal systems or organisational information against any malicious attacks.

©IJRASET: All Rights are Reserved

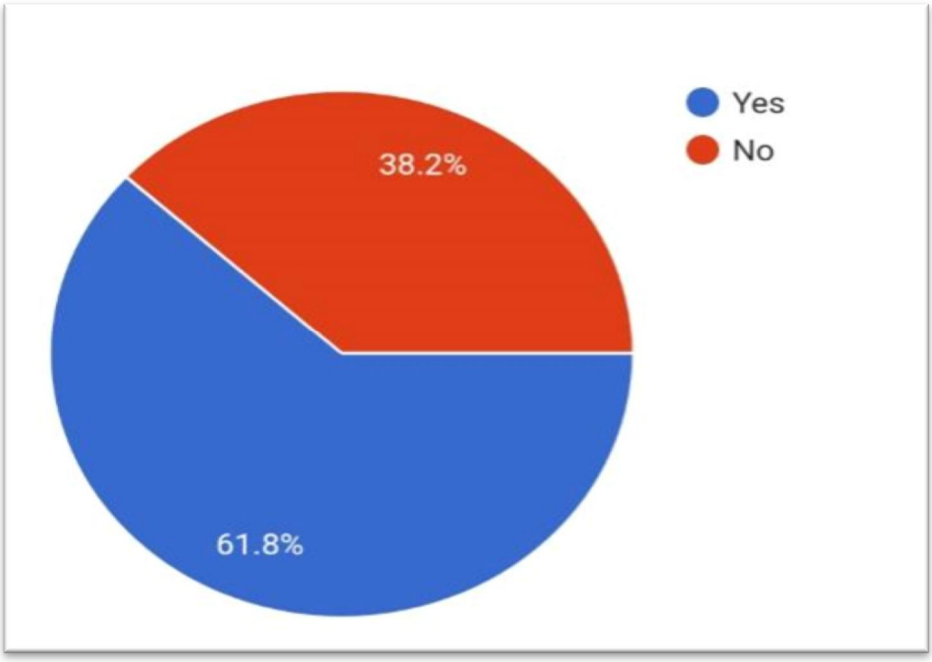


Fig 1. Pie chart representation

People responses on two parameters on spending money for protecting the data i.e. YES/NO.

VI. RESULT

From the experiment it is proved that population need special tool to detect suspicious activities or threats. Since nowadays such activities are increasing day by day people's are more conscious about their data. By applying Chi-square test on quantitative data proposed hypothesis is accepted . Also from the analysis it is realized that population are secure about theirs personal as well as organizational information.

VII. CONCLUSION

Majority of the population think that the Internet is not safe because of the cyberbullying and malicious activities. So according to the experiment it is concluded that population wants to protect themselves from such activities by using the software or tool like honeypots to detect the threat .. So honeypot is the best tool to protect our data against any loss. The article is also summarizes that, nowadays people's are more fretting about their data security for that they wants honeypot to detect cyber attacks or they can pay against any suspicious activities.

VIII. ACKNOWLEDGEMENT

A special thank of gratitude to prof. Swapna Nikale, Department of Information Technology B. k. Birla College (Autonomous) Kalyan.

REFERENCES

[1] Gelenbe, E., Lyberopoulos, G., Baltatu, M., Gorbil, G., Tzovaras, D., Liebergeld, S., & Garcia, D. (2013). Security for smart mobile networks: The NEMESYS approach. Security for Smart Mobile Networks: The NEMESYS Approach, 1–25. https://doi.org/10.1109/GHTCE.2013.6767242

[2] Ahmed, H. . m. o. h. s. i. n., Hassan, N. . f. l. a. i. h., & Fahad, A. (2017). Designing a smartphone honeypot system using performance counters. Designing a Smartphone Honeypot System Using Performance Counters, 1–7. http://www.journals.elsevier.com/karbala-international-journal-of-modern-science

[3] Gelenbe, E., Gorbil, G., Oklander, B., & Abdelrahman, O. (2013). Mobile network anomaly detection and mitigation: The NEMESYS approach. Mobile Network Anomaly Detection and Mitigation: The NEMESYS Approach, 7–42. https://doi.org/10.1007/978-3-319-0160

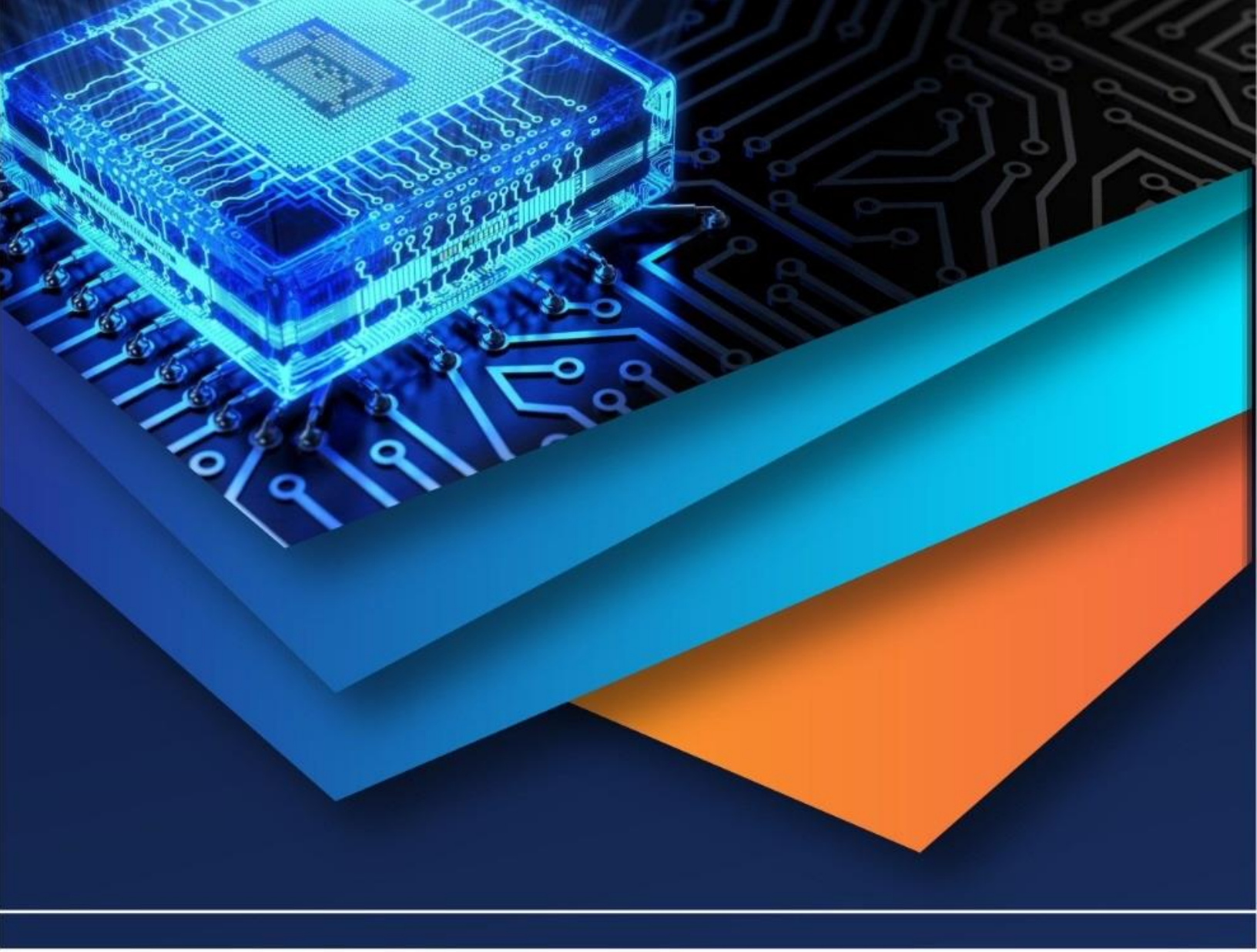
[4] Gelende, E., Gorbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., & Lyberopoulos, G. (2012). NEMESYS: Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem. NEMESYS: Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem, 1–9. http://www.nemesys-project.eu/nemesys/index.html

[5] Kleber, S., Kopp, H., & Kargl, F. (2018). NEMESYS: Network Message Syntax Reverse Engineering by Analysis of the Intrinsic Structure of Individual Messages. NEMESYS: Network Message Syntax Reverse Engineering by Analysis of the Intrinsic Structure of Individual Messages, 1–12. https://www.usenix.org/conference/woot18/presentation/kleber

©IJRASET: All Rights are Reserved

[6] Ahmed Salman, H. . m. o. h. s. i. n., Fahad, A., & Hassan, N. (2013). A Survey on Smartphone Honeypot. A Survey on Smartphone Honeypot, 11(4), 2476–2480. https://doi.org/10.24297/ijct.v11i4.3131
[7] Krishnamurthy, B. (2004). Mo honk: Mobile honeypots to trace unwanted traffic early. Mo honk: Mobile Honeypots to Trace Unwanted Traffic Early, 1–6. https://doi.org/10.1145/1016687.1016696
[8] Anagnostakisy, K. G., Sidiroglouz, S., Akritidis, P., Xindis, K., Markatos, E., & Keromytisz, A. D. (2005). Detecting Targeted Attacks Using Shadow Honeypots. Detecting Targeted Attacks Using Shadow Honeypots, 129–144. https://www.researchgate.net/publication/243787508_AD_Detecting_Targetted_Attacks_Using_Shadow_Honeypots
[9] Mokulbe, I., & Adams, M. (2007). Honeypots: Concepts, Approaches, and Challenges. Honeypots: Concepts, Approaches, and Challenges, 321–326. https://doi.org/10.1145/1233341.1233399
[10] Zhug, J., Holz, T., Han, X., & Song, C. (2007). Collecting Autonomous Spreading Malware Using High-Interaction Honeypots. Collecting Autonomous Spreading Malware Using High-Interaction Honeypots, 438–451. https://doi.org/10.1007/978-3-540-77048-0_34
[11] Proxos, N. (2003). Honeyed: A Virtual Honeypot Daemon (Extended Abstract). Honeyed: A Virtual Honeypot Daemon (Extended Abstract), 1–7. https://www.researchgate.net/publication/250395424_Honeyd_A_Virtual_Honeypot_Daemon_Extended_Abstract
[12] Yehneswaran, V., Barford, P., & Paxson, V. (2005). Using Honey nets for Internet Situational Awareness. Using Honeynets for Internet Situational Awareness, 1–6. https://www.researchgate.net/publication/248269092_Using_Honeynets_for_Internet_Situational_Awarenessand
[13] J, J., & Muthukumar, D. B. (2015). Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach. Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach, 338–346. https://doi.org/10.1016/j.procs.2015.04.191
[14] Kreibich, C., & Crowcroft, J. (2004). Honeycomb – Creating Intrusion Detection Signatures Using Honeypots. Honeycomb – Creating Intrusion Detection Signatures Using Honeypots, 51–56. https://www.researchgate.net/publication/220195508_Honeycomb_-_Creating_Intrusion_Detection_Signatures_Using_Honeypots
[15] Song, J., Takakura, H., Okabe, Y., Inoue, D., Eto, M., & Nakao, K. (2010). A Comparative Study of Unsupervised Anomaly Detection Techniques Using Honeypot Data. A Comparative Study of Unsupervised Anomaly Detection Techniques Using Honeypot Data, 2544–2554. https://doi.org/10.1587/transinf.E93.D.2544
[16] Bhagat, N., & Arora, B. (2018). HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot. HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot, . https://doi.org/10.1109/PDGC.2018.8745761
[17] Lee, S., Kim, G., & Kim, S. (2011). Self-adaptive and dynamic clustering for online anomaly detection. Self-Adaptive and Dynamic Clustering for Online Anomaly Detection, 14891–14898. https://doi.org/10.1016/j.eswa.2011.05.058
[18] Boukela, L., Zhang, G., Bouzefrane, S., & Junlong, Z. (2020). An outlier ensemble for unsupervised anomaly detection in honeypots data. An Outlier Ensemble for Unsupervised Anomaly Detection in Honeypots Data, 743–758. https://doi.org/10.3233/IDA-194656
[19] Honeypots: Tracking Hacker By Lance Spitzner Publisher: Addison Wesley
[20] Cliff Stoll. 1990. The Cuckoo's Egg. New York, New York: Pocket Books Nonfiction
[21]

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)