Detection and Analysis of Active Attacks using Honeypot

Waqas Ahmad
Department of Software Engineering
Lahore Garrison University
Lahore, Pakistan

Muhammad Arsalan Raza
Department of Computer Science
Lahore Garrison University
Lahore, Pakistan

Sabreena Nawaz
Department of Information Technology
Lahore Garrison University
Lahore, Pakistan

Farhana Waqas
O-Levels Section
Beaconhouse School System
Gujrat, Pakistan

ABSTRACT
Honeypots are computer systems specifically deployed to deceive attackers so that they consider them legitimate computers. Honeypots are actually a trap to trick the attackers so that we can learn about their behavior and the attack methods they use. Security experts collect all the relevant information about attack techniques and behavior and take firm actions to strengthen security measures. Although another technique is also being used which is Intrusion Detection and Prevention System (IDPS), but it generates false positives and false negatives, which is a limitation of IDPS. Therefore, to know the behavior, methods, techniques, and signatures of an attacker, the Dionaea honeypot system is used to collect the information regarding cyber-attacks, proving it a more useful way rather than previous traditional methods. Attacks that were captured by the honeypot software reveal the source IP addresses of the attackers and the target host which became the victim of attacks.

General Terms
Information Security

Keywords
Attack, Exploit, Honeypot, Patterns

1. INTRODUCTION
An information system resource called a honeypot is one whose value comes from being used illegally or unauthorizedly [1]. Any interaction with a honeypot is assumed to have malicious intent because attacker thinks it is a vulnerable system and it can be attacked easily. As techniques of network protection, firewalls and Intrusion Detection and Prevention Systems (IDPS) are well known. All of these techniques have some limitations. But honeypot offers an alternative strategy, it traps the attackers because of its deceiving nature. In [2] firewall would allow only authorized traffic to enter or leave the private network, but it gathers large amount of data that an administrator would find prohibitive to analyze. On the other hand, a honeypot will only collect the data of log attacks to a target host. It is believed that the small data sets in the analysis of log attacks using honeypots are easier to manage and analyze, plus the intrusion detection and prevention system is not a reliable security measure because IDPS generates false-positive warnings that needs to be resolved. Apart from false positives, IDPS also generates false negatives alarms, which is of course one of the research problems in IDPS. That is why honeypot scheme is used for the purpose of analysis of compromised hosts in this research paper. As already said before, that any interaction with a honeypot is considered as a harmful and malicious activity that warrants further examination and deep analysis of source attacker and pattern of the attack. A honeypot is used to see if intruders are testing the security of your system by invading it, and the log files tell the detail of different patterns used by the attackers [3].

2. LITERATURE REVIEW
Authors in their study [4] have done comprehensive review of cyberattacks detection using honeypot system and proved worthwhile. They also concluded that honeypot and machine learning can be useful in predicting and building strong models for suspicious profiles. The study in [5] focused on critical issues relating to internet of things (IoT) technology. They used reinforcement learning (RL) to design a honeypot to detect attacks that can occur due to DDoS and Man in the Middle attack. They found that a honeypot designed with reinforcement learning can detect up to 99.96% of the attacks and outperform previous honeypots in terms of performance. Another study in [6] has shown that using honeypot is far better than using firewall and IDPS, but if honeypot is implemented with IDPS, this can reduce false positives and false negatives to some extent. The study in [7] it has been observed that using honeypot decoy system, we can protect our systems from the distributed denial of service attacks. They analyzed this thing by using simulation. Another study in [8] found some discrepancies in intrusion detection and prevention system to catch the attack signatures used by the attackers, and concluded that it is not a reliable system and it generates false positives and false negatives. The study in [9] also tried honeypot programs to trick the attackers and eventually found it as a reliable method to learn the different patterns of the attackers. Also, they found that by using honeypot system, we can tighten our security of the systems. Similarly, they worked on to detect the anomalies in a network. They have studied previous techniques to detect the anomalies, but later on suggested entropy-based anomaly-based detection in a network. The study in [10] proposed a kernel-based honeypot hiding technique using rootkit, so that attackers can never detect a honeypot system. In another study in [11] authors established SSH and Telnet honeypot using cowrie software. In this study, it was shown that in these days, attackers use zero-day attacks to counter honeypots, which is a concern for the security professionals. Attackers are using SSH and Telnet methods to tackle with honeypots and to attack the systems remotely. In the recent study by authors in [12], has shown that ChatGPT despite of its weaknesses has the tendency to become a reliable honeypot system in future cyberworld, and it will be an innovative approach in terms of honeypot. Another study in [13] a honeypot shadow server (Honeyd) has been discussed which resembles like a real server. In this research paper, analysis and implementation of Honeyd was done to enhance security systems. In latest research in [14], they

conducted a meta-analysis of developments in honeypot systems by doing deep study of previous research papers, and ultimately found honeypot systems and Honeyd as the most trustworthy technique in identifying the latest attack methods and to secure the networks. In the study in [15] a honey pot game theoretical model is used to investigate the offensive and defensive interactions. Authors were successful in providing an optimized defensive strategy in case of honeypots.

3. HONEYPOT SOFTWARES

There are various tools that are used for the purpose of data collection by creating a decoy system or network in order to attract and monitor cyber-attacks. All these tools are known as honeypot software. Organizations or individuals can use any of this software to make honeypot for keeping their network safe by analyzing, predicting, and knowing the method, signatures, and techniques of the cyber attackers. Following are the honeypot software that collect data, and afterwards analyze the collected data. The detail and the name of these data collection software are mentioned below.

3.1 Back Officer Friendly

Back Officer Friendly is a tool that is used in the field of cybersecurity to create and manage honeypots. Honeypots are decoy systems that are designed to look and act like real systems in order to attract and deceive potential attackers. By using a honeypot, cybersecurity professionals can gain valuable insights into an attacker's methods and motives, as well as gather information that can be used to improve the security of real systems. Back Officer Friendly is a tool that can help in the deployment and management of honeypots, making it easier for security professionals to use this valuable technique to protect their organizations. Below is the figure no. 1 that shows the warnings window of Back Officer friendly, to get some idea how this tool actually looks like [16].

Figure 1: Warnings Window in Back Officer

BOF has another window as well, which is the log output window, and this window is more advantageous in terms of attack examining on the system as compared to BOF alarm window. Because alarm window requires the continuous monitoring from the network manager. Below is the figure no. 2 that shows the screenshot of log output window of the BOF below [16].

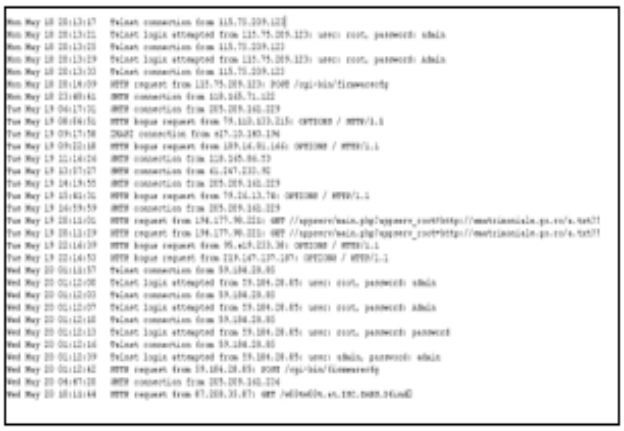

Figure 2: Log output in Back Officer Friendly

3.2 HoneyBOT Software

HoneyBOT is also a powerful tool that automates the deployment and management of honeypots, making it easier for security professionals to use this technique to protect their organizations. Although it is not an open-source application, there is still a free trial version available online. It is very easy to install. Initially it picks up a lot of background noise traffic, but then eventually it becomes stable. It has a feature in which we can disable the more occasionally used ports, leaving only the uncommon ports to be watched for strange behavior. Below is the figure no. 3 that shows the graphical user interface of honeyBOT tool [17].

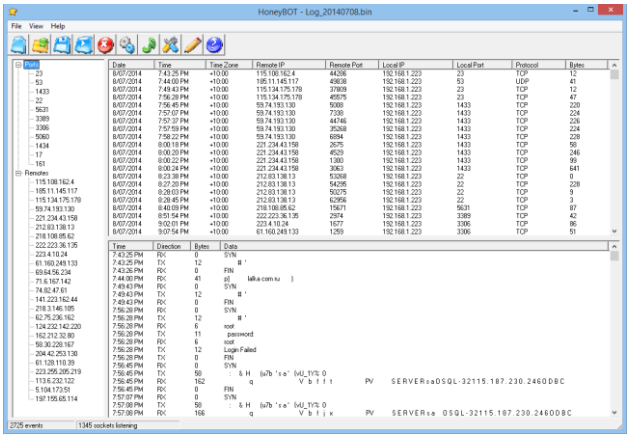

Figure 3: Graphical User Interface of HoneyBOT

3.3 Nepenthes Software

It is an automated framework for malware collection. There are two different nepenthes honeypots i.e., low interaction honeypots and high interaction honeypots. The benefit of low interaction nepenthes honeypot is that it can easily be installed and configured. Also, it requires less resources. Moreover, it has much faster speed than high interaction honeypots and it provides emulated network services to the intruders. It also has the ability to quickly tell the network manager for any malicious activity. It also assists in removing the malwares. It has various modules which are vulnerability module, shellcode emulators, download module and submission module. It may also be used in combination of an IDPS for better results [18]. Below is the figure 4 that shows the screenshot of a log output window.

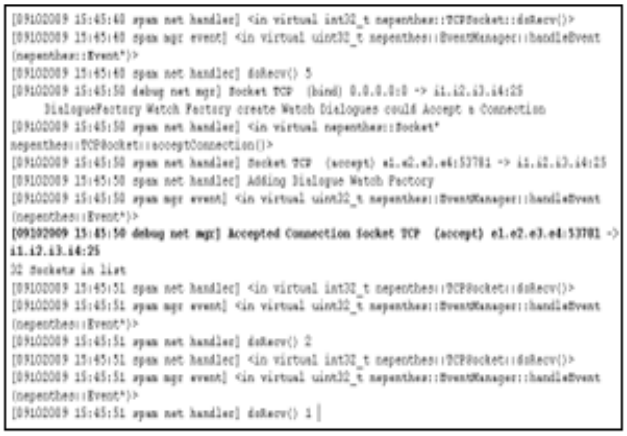

Figure 4: Log output in Nepenthes

3.4 Dionaea Software

It was released as "Nepenthes" replacement or successor and it has embedded python as a scripting language. It is also used to detect, malwares, and payloads. Everyone can easily download this tool from this link https://github.com/DinoTools/dionaea. It also has the ability to emulate vulnerable windows and can capture malware which was sent to exploit the system. New version of Dionaea gives the graphical user interface to the users. Below is the figure 5 that shows the screenshot of a graphical user interface of Dionaea [19].

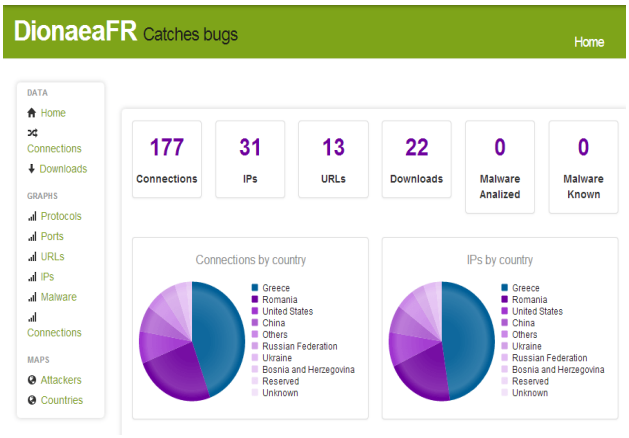

Figure 5: Graphical User Interface of Dionaea

3.5 Kippo Software

Kippo is not a low interaction honeypot, rather it is a medium interaction honeypot. It mainly targets on the log of brute force attacks and most importantly on the whole shell interaction by the attacker. Kippo can be downloaded from the following link https://github.com/desaster/kippo. It is also known as SSH honeypot. Whenever an attacker tries to seize control of the SSH, Kippo captures the whole shell interaction of the attacker. Below is the figure 6 that shows the exact locations of source IP addresses, from where the attackers have launched their malicious intents [20].

Figure 6: Exact Locations of Cyberattacks

3.6 Honeyd Software

Honeyd is a free and open-source honeypot software that allows users to emulate multiple operating systems and services on a network to attract and monitor potential attackers. The software works by creating virtual machines, known as honeypots, which appear to be vulnerable and easily exploitable to attackers. When an attacker attempts to exploit the honeypot, Honeyd captures and logs the attack, providing valuable insights into attacker behavior and techniques. Honeyd is highly customizable, allowing users to configure a wide range of virtual hosts and services, making it an effective tool for both research and security purposes. While setting up and maintaining a Honeyd system can be complex, it is a powerful and valuable tool for understanding and defending against cyber threats. Below is the figure no. 7 that shows the port scanning of the virtual Honeyd [21].

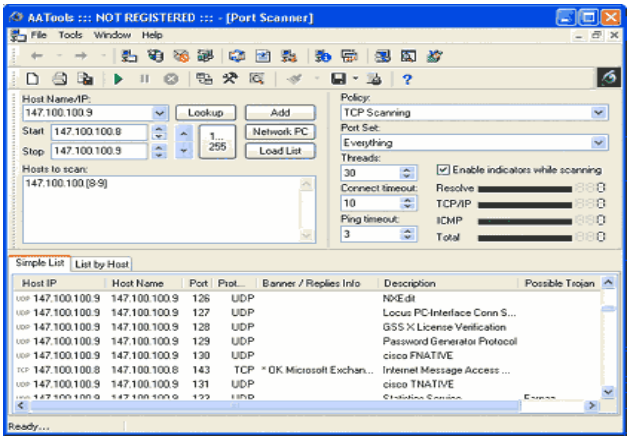

Figure 7: Virtual Honeyd Port Scanner

4. RESULTS AND DISCUSSION

In this manuscript, Dionaea honeypot was selected to capture, predict, and learn about the attack methods used by the attackers. As already discussed before, it is a low interaction honeypot and the performance of low interaction honeypots are better than medium interaction honeypots in certain conditions. It can easily emulate vulnerable windows. In this study Dionaea honeypot system was built using a bridged network setup that uses the capabilities of virtual machine and a virtual version of Ubuntu 12.04 which runs under VMware Workstation. After having done with the installation of Ubuntu, modern honey network platform was installed and default settings were used for the set up. The demilitarized zone was then used to link the honeypot machine, which was given a public address. Once the modern

honeypot network platform is functional and operational, a variety of scripts may be deployed underneath it. The command will be entered on Ubuntu command line using a Dionaea honeypot. It will start the installation of a honeypot for Dionaea. Once a honeypot has been fully installed, it must wait to see whether an attack is captured. However, it can be seen by running a Nmap scan against the modern honeypot network system's IP address [22], it was found that many attacks were being launched. Below is the figure no. 8 that shows a live map representation of the world where cyber-attacks are occurring.

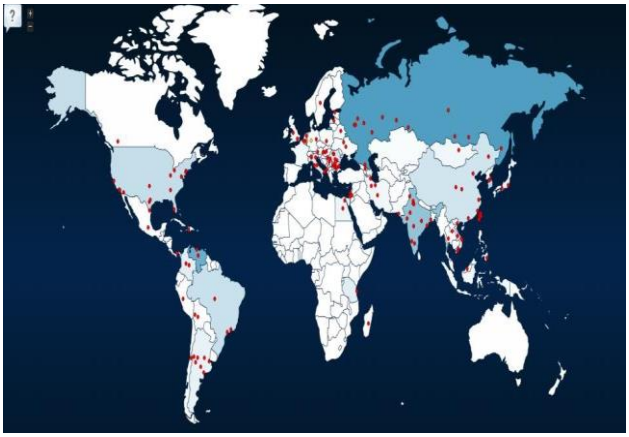

Figure 8: Live Map of Active Attacks

4.1 Analysis of Source IP Addresses

After finishing with the complete set up and installation of Ubuntu and Dionaea honeypot, it was found that different source IP addresses were trying to attack the demilitarized zone honeypot, which can also be seen in figure no. 8. Red dots represent different regions of the world, where cyber-attacks are happening. It has been observed, that there was a specific IP address that tried to attack the demilitarized zone on frequent basis, courtesy Dionaea honeypot. According to the analysis performed, it was found that 13790 attempts were made by the IP address i.e., 188.165.238.186 that attacked the demilitarized zone of honeypot. The second most attempts i.e., 500 attempts, were made by another IP address 31.223.187.172. Out of twenty IP addresses found, the first IP address was significant. Below is the figure no. 9 that shows the results of those IP address that attacked the demilitarized zone of honeypot.

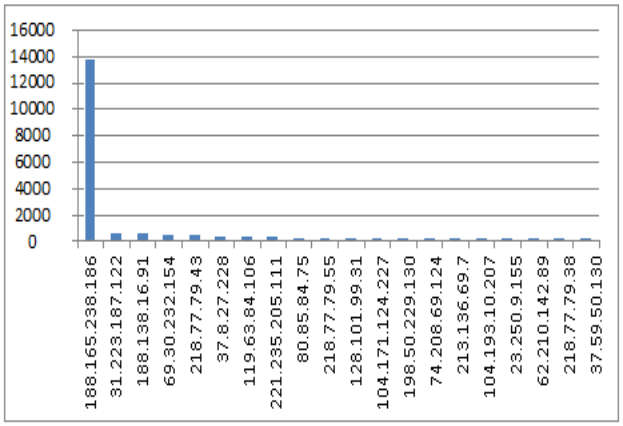

Figure 9: IP Address that Attacked DMZ Frequently

In another figure it is clearly visible that among various ports that were attacked by the attackers, port number 5060 was the one which was attacked large number of times. This port number 5060 is the port number of session initiation protocol (SIP) port. Graph shows that this port was attacked almost 21000 times. The names of other ports that were under attack are Microsoft Directory Services, Secure Shell Remote Login Protocol and Telnet. The number for these ports is 445, 22, and 23 respectively. Below is the figure no. 10 that shows the results of the different ports that were attacked by the attackers.

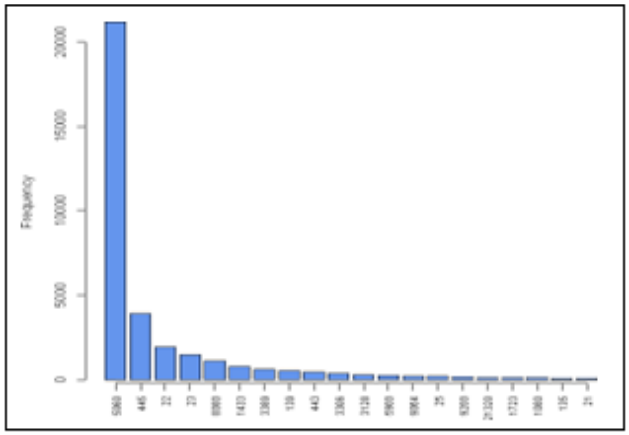

Figure 10: Attack Frequency on Ports

5. CONCLUSION

Many honeypot deployments can be done, but we chose Dionaea because it allows to collect the large amount of data set to analyze the source IP addresses from where the attack has been launched. Honeypot system and Honeyd system are useful because they indict number of attacks that an IP address attracts, and focuses on high level of security for the networks. Log information collected from the honeypot system provides valuable information to the network managers who are managing big networks. In this way, network managers can harden the security of the networks. Our manuscript also strengthens the concept of using the honeypot system, because it is a good way to lure the attackers to enter into a trap. By doing so, organizations can collect, understand the attack information, patten and motive of the intruder. We can also share it with other organizations, keeping it available for everyone. Hence making the internetworking more secure and preventing the attackers in succeeding in their malicious intents.

6. ACKNOWLEDGMENT

We would like to thank our mentor Dr. Khalid Masood, who is working as an associate professor in the department of software engineering at Lahore garrison university. He has guided us and motivated us in every step of this research. We also thank the chairperson of the information technology department, Dr. Ahmed Naeem for initial review of this manuscript, although any errors are our own and should not tarnish the reputations and credibility of these esteemed persons.

7. REFERENCES

[1] Priya, V. D., & Chakkaravarthy, S. S. (2023). Containerized cloud-based honeypot deception for tracking attackers. Scientific Reports, 13(1), 1437.

[2] Hussein, M. A. (2023). A Proposed Multi-Layer Firewall to Improve the Security of Software Defined Networks. International Journal of Interactive Mobile Technologies, 17(2).

[3] Jadhav, Y. C., Sable, A., Suresh, M., & Hanawal, M. K.

(2023, January). Securing Containers: Honeypots for Analysing Container Attacks. In 2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS) (pp. 225-227). IEEE.

[4] Amal, M. R., & Venkadesh, P. (2022). Review of cyber attack detection: Honeypot system. Webology, 19(1), 5497-5514.

[5] Pashaei, A., Akbari, M. E., Lighvan, M. Z., & Charmin, A. (2022). Early Intrusion Detection System using honeypot for industrial control networks. Results in Engineering, 16, 100576.

[6] AlZoubi, W., & Alrashdan, M. (2022). The effect of using honeypot network on system security. International Journal of Data and Network Science, 6(4), 1413-1418.

[7] Wang, X., Guo, N., Gao, F., & Feng, J. (2019). Distributed denial of service attack defence simulation based on honeynet technology. Journal of Ambient Intelligence and Humanized Computing, 1-16.

[8] Rabadia, P. N. (2018). Extraction of patterns in selected network traffic for a precise and efficient intrusion detection approach.

[9] Shukla, A. S., & Maurya, R. (2018). Entropy-based anomaly detection in a network. Wireless Personal Communications, 99(4), 1487-1501.

[10] Mohammadzad, M., & Karimpour, J. (2023). Using rootkits hiding techniques to conceal honeypot functionality. Journal of Network and Computer Applications, 103606.

[11] Başer, M., Güven, E. Y., & Aydın, M. A. (2021, September). SSH and Telnet Protocols Attack Analysis Using Honeypot Technique: Analysis of SSH AND TELNET Honeypot. In 2021 6th International Conference on Computer Science and Engineering (UBMK) (pp. 806-811). IEEE.

[12] McKee, F., & Noever, D. (2023). Chatbots in a Honeypot World. arXiv preprint arXiv:2301.03771.

[13] Nasution, A. M., Zarlis, M., & Suherman, S. (2021). Analysis and implementation of honeyd as a low-interaction honeypot in enhancing security systems. Randwick International of Social Science Journal, 2(1), 124-135.

[14] Ikuomenisan, G., & Morgan, Y. (2022). Meta-Review of Recent and Landmark Honeypot Research and Surveys. Journal of Information Security, 13(4), 181-209.

[15] Tian, W., Ji, X. P., Liu, W., Zhai, J., Liu, G., Dai, Y., & Huang, S. (2019). Honeypot game-theoretical model for defending against APT attacks with limited resources in cyber-physical systems. Etri Journal, 41(5), 585-598.

[16] Tiwari, A. (2022). Comparitive Analysis of Various Honeypot Tools on the Basis of Their Classification and Features. Available at SSRN 4306515.

[17] Irvene, C., Formby, D., Litchfield, S., & Beyah, R. (2017). HoneyBot: A honeypot for robotic systems. Proceedings of the IEEE, 106(1), 61-70.

[18] Rustamovna, S. H., & Azimjon o'g'li, B. S. (2022). IN THE FIELD OF CYBER-SECURITY AN INTRUSION DETECTION SYSTEM BASED ON HONEYPOT TECHNOLOGY. Conferencea, 348-352.

[19] Franzen, F., Steger, L., Zirngibl, J., & Sattler, P. (2022, June). Looking for Honey Once Again: Detecting RDP and SMB Honeypots on the Internet. In 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 266-277). IEEE.

[20] Dowling, S., Schukat, M., & Barrett, E. (2020). New framework for adaptive and agile honeypots. ETRI Journal, 42(6), 965-975.

[21] Foo, C. S. (2019). Network Isolation and Security Using Honeypot (Doctoral dissertation, UTAR).

[22] Kelly, C., Pitropakis, N., Mylonas, A., McKeown, S., & Buchanan, W. J. (2021). A comparative analysis of honeypots on different cloud platforms. Sensors, 21(7), 2433.