Instituto Politécnico de Viana do Castelo
Escola Superior de Tecnologia e Gestão

Year 2022/2023 | Graduation Computer Engineering | Subject Cryptography and Systems Security

Students Célio Pina and Rúben da Luz | Supervision Pedro Pinto, Hugo Almeida

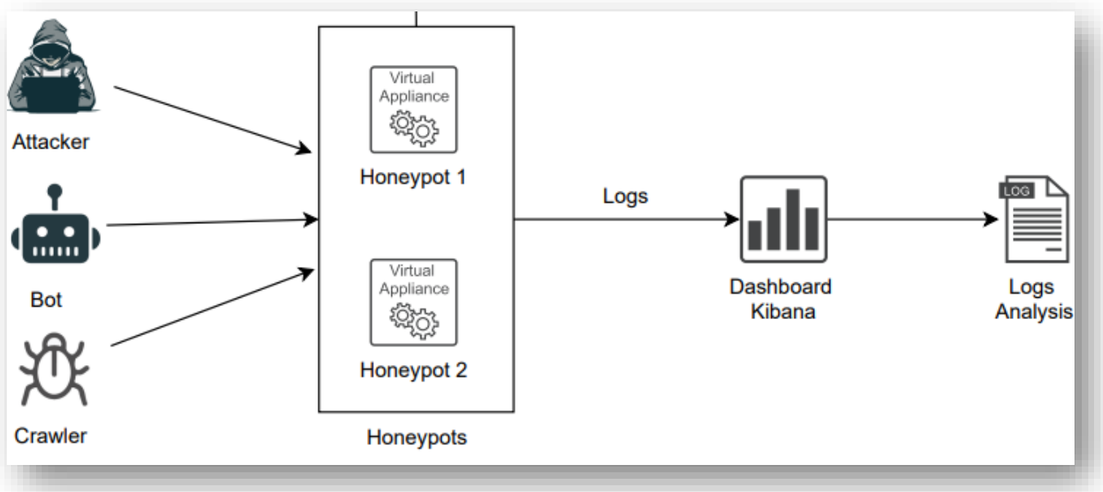
Hackers Activity on the Internet

INTRODUCTION

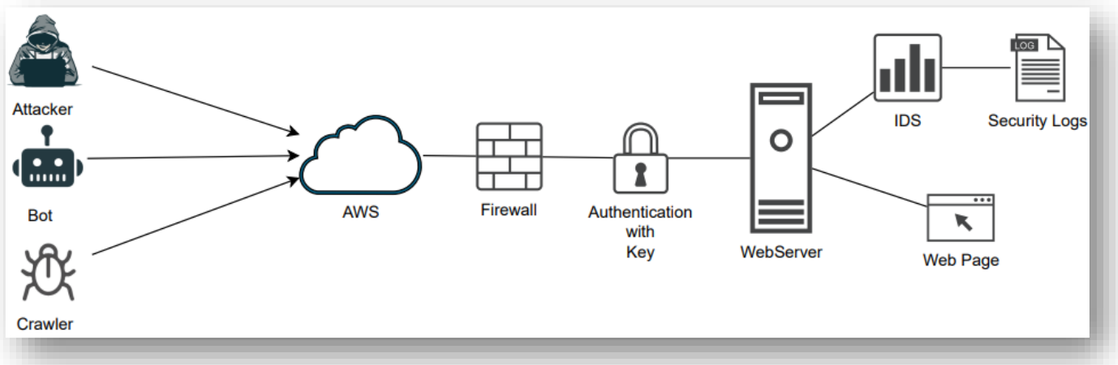
As technological advancements progress and our reliance on the Internet deepens, the rise in hacking activity has emerged as a pressing concern in contemporary times. This research aims to analyze the activities of hackers on the internet and assess the effectiveness of using honeypots in the AWS cloud as a proactive security measure, attracting hackers and gathering valuable data about their activities. By deploying and configuring two low-in honeypots in different regions in the AWS cloud, it becomes possible to monitor and analyze the behavior of hackers, identify attack patterns, and develop more effective security solutions. This study aims to contribute to the understanding of hacker activity and enhance the protection of systems and networks against cyber threats.

WORK

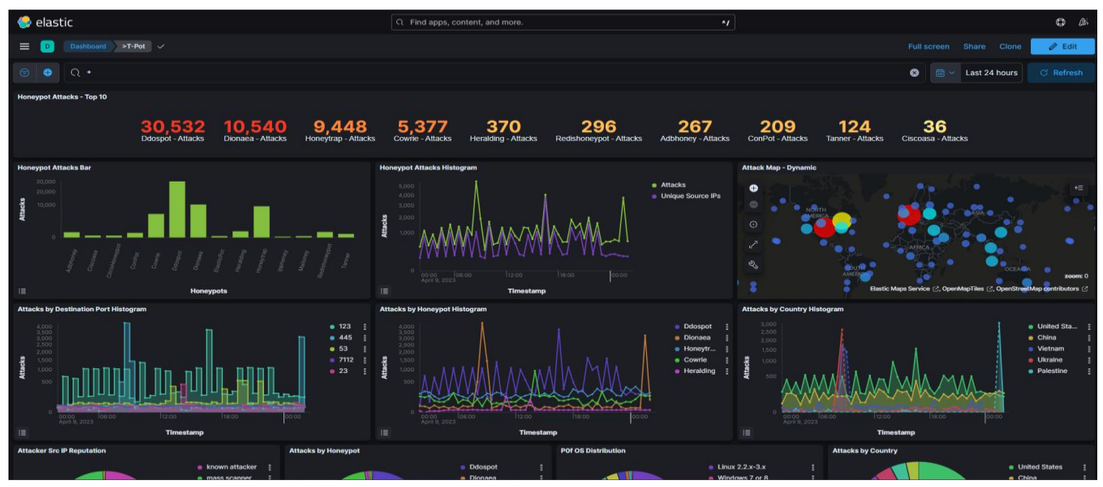
Our main objective is to deploy two honeypots in separate locations within the AWS cloud service. By collecting and analyzing data, we aim to study various aspects of attacks, including their origin, frequency, and techniques. This information, visualized through the Kibana framework as shown in the figure, will enable us to develop effective defense strategies for protecting real servers against these potential threats.



In our project, we aim to demonstrate and propose a safer infrastructure for deployment in the cloud. Through practical testing and research results, we suggest security measures based on good practices in cloud computing. The proposed framework, depicted in Figure 9, showcases the implementation of a firewall with key pair authentication and public key cryptography to protect a Software as a Service (SaaS) provided by a cybersecurity company in the AWS cloud. Additionally, we emphasize the importance of monitoring server security logs to ensure ongoing security and vulnerability management.

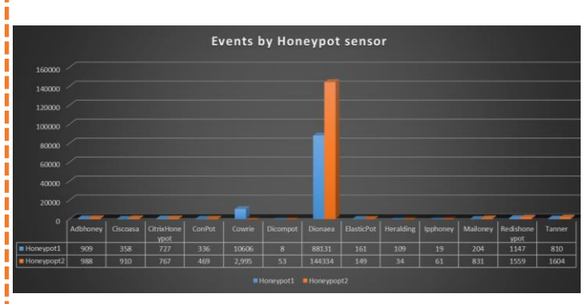


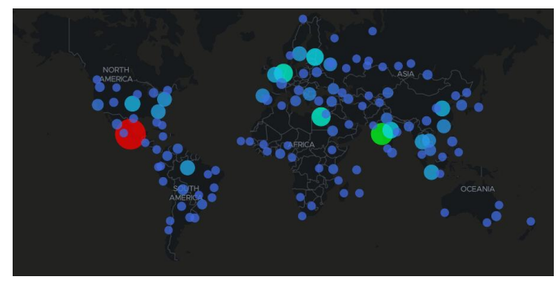
After installation, we accessed the honeypots dashboard using the URL format: https://<instance_public_ip>:64297. Login and choose Kibana. Select the T-pot dashboard for comprehensive analysis of all sensors, as shown in figure:



RESULTS

We had a total of 258 279 events recorded in both honeypots, as can be seen in figure bellow on the left, and on the right an Attack map that show that we received attacks from all over the globe.





Mexico that registered a total of 36731 attacks on honeypot 1, followed by India with 19842 attacks. On honeypot 2 we can see a completely different scenario as Vietnam and Egypt were the ones with more attacks with 21571 and 15767 , respectively. The most attacked port was port 445, that is used by SMB, a network file sharing protocol, this port is vulnerable to security assaults, according to security researchers, and should be deactivated or well protected. The GET method was the most use in HTTP request, with attackers making 8562 GET requests. This method is used to retrieve data from a specified resource. The CVE-2020-11899 exploit was prominently employed. This particular exploit targets an improper input validation vulnerability in the IPv6 component, which allows an unauthorized network attacker to send a malicious request. Therefore, the target device may experience an out-of-bounds read, potentially leading to a denial-of-service condition.

CONCLUSIONS

Honeypots play a crucial role in understanding attackers by attracting and studying their behavior. Our comprehensive analysis provides valuable insights into threat origins, attack frequencies, interaction patterns, and attack types in cloud environments. These findings contribute to the development of improved detection and defense strategies. However, it is important to address the limitations arising from default templates and short experiment periods to ensure more accurate results. By leveraging our research, organizations can enhance their security measures and better protect their computing infrastructures in the cloud.

REFERENCES & LINKS

1. Islam, “Know Your Enemy: Analysing Cyberthreats Against Industrial Control Systems Using Honeypot,” en, in 2019 IEEE International
2. Dhaka, Bangladesh: IEEE, Nov. 2019, pp. 151–154, ISBN: 978-1-72815-852-5. DOI: 10 . 1109 /RAAICON48939 . 2019 . 69. [Online]. Available:
3. [4] S. M. Z. U. Rashid, A. Haq, S. T. Hasan, M. H
4. Furhad, M. Ahmed, and A. S. S. M. Barkat Ullah,“Faking Smart Industry: A Honeypot-Driven Approach for Exploring Cyber Security Threat Landscape,” en, in Cognitive Radio Oriented WirelessNetworks and Wireless Internet, H. Jin, C. Liu,