Chad Ballay

CYBR410

10/12/2020

Week 7 -Module 2

1. **Why would a database administrator set up a honeypot?**

To gain even greater insight to the status and security of his database infrastructure. Plumbers use a similar approach with dyes to attempt to identify where a leak is originating. Doctors will use a similar approach with mapping blood flows. The concept is the same. Make an unseen flow of information visible so that it can be detected through easier means. In the case of databases the idea would be that this would provide a means to identify when information had been exfiltrated. Or that during the infiltration stage that these targets would bubble up as the most likely of targets therefore they are to be monitored more diligently. (Jr., n.d.)

1. **What role does a firewall play in a honey pot design?**

The honey pot has to look and feel like a real system while having a thoroughly monitored existence. Often times this means that the network layer around the honey pot is actually where the majority of the monitoring is being done.

For databases this network layer monitoring will often inspect the traffic for the database and infer the intent. This is possible due to SQL being a thoroughly mapped domain. Upon inspection if enough suspicion is raised the firewall could seamlessly redirect the identified traffic into a higher monitored alleyway. (Wegerer & Tjoa, 2016)

A curated list is maintained here but it is prone to being updated as advancements and time change the landscape. <https://github.com/paralax/awesome-honeypots#honeypots>

1. **What is the difference between hashing a password and encrypting it?**

Hashing is a mathematical transformation that is one way by definition. The original state of the data cannot be computed by working backwards from the end product. So when the algorithm is worked upon the data a unique to that specific instance of data is the result but at no point can you be given a result and told to work backwards to the starting point. (ircmaxell, n.d.)

Encryption is a mathematical transformation that is two way. The original and cipher text can be universally reached if the user knows the mechanism and the key used. This means that once I give you the pieces of cipher text and key, you could work backwards to the original text I encrypted. Universally. (BIGinsight: The Difference Between Hashing and Encryption, n.d.)

# Works Cited

*Canarytokens.org - Quick, Free, Detection for the Masses*. (n.d.). Retrieved from Thinkst: https://blog.thinkst.com/p/canarytokensorg-quick-free-detection.html

*BIGinsight: The Difference Between Hashing and Encryption*. (n.d.). Retrieved from Medium: https://medium.com/bigtoken/biginsight-the-difference-between-hashing-and-encryption-5c3d3942a259

Burn, J. (n.d.). *The Importance of Resilience Testing and Observability*. Retrieved from The New Stack: https://thenewstack.io/the-importance-of-resilience-testing-and-observability/

*First-Mover Advantage*. (n.d.). Retrieved from WIkepidea: https://en.wikipedia.org/wiki/First-mover\_advantage

Hospelhorn, S. (n.d.). *What is The Cyber Kill Chain and How to Use it Effectively*. Retrieved from Varonis: https://www.varonis.com/blog/cyber-kill-chain/

*Inference Attack*. (n.d.). Retrieved from Cybary: https://www.cybrary.it/glossary/i-the-glossary/inference-attack/

*Infrastructure as Code*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Infrastructure\_as\_code

ircmaxell. (n.d.). *Fundamental difference between Hashing and Encryption algorithms* . Retrieved from StackOverflow: https://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-and-encryption-algorithms

Jr., C. F. (n.d.). *How to Comprehend the Buzz About Honeypots*. Retrieved from DarkReading: https://www.darkreading.com/edge/theedge/how-to-comprehend-the-buzz-about-honeypots/b/d-id/1336788

Sgobe, T. (n.d.). *Installation and Oracle Database Creation in Silent Mode*. Retrieved from EzDBA - BLOG: https://ezdba.wordpress.com/2016/09/01/installation-and-oracle-database-creation-in-silent-mode/

Shroff, A. (n.d.). *Oracle Developer's blog*. Retrieved from Infrastructure as Code using Terraform on Oracle Developer Cloud: https://blogs.oracle.com/developers/infrastructure-as-code-using-terraform-on-oracle-developer-cloud

Wegerer, M., & Tjoa, S. (2016). Defeating the Database Adversary Using Deception - A MySQL Database Honeypot. *2016 International Conference on Software Security and Assurance (ICSSA)*, 6-10.