Jason Hodge

Lab 03 – Open Source Intelligence Gathering

October 25, 2023

OSINT Literature Review

The open source (OSINT) framework is an accumulation of multiple methods, tools, and resources used to discover public information about any given organization. Through utilizing open-source methods of gaining publicly available knowledge, anyone can learn about a system for both good and bad purposes. Whether it is to see what information is available about their own organization or to learn about an organization one would like to learn more about. Some information is rather basic while other bits of information could be used maliciously to get into open vulnerable areas in an organizations system. Throughout history, as powerful search engines continued to grow so did the power to gain open-source knowledge. Thus, this publicly available information has both good intensions and bad intensions, which raise various privacy concerns.

Numerous cybersecurity professionals utilize open-source search engines and tools before they start diving into running penetration testing tools to identify vulnerabilities within systems. Furthermore, information discovered can be utilized to help protect and fight against cybercrime and suspicious actors and groups. Through the use of surveillance technologies such as “Cyber Threat Intelligence (CTI), which focuses on the detection and analysis of cyber threats, and risk mitigation systems, which work towards identifying actors and groups” (Riebe, T., Biselli, T., Kaufhold, M.-A., & Reuter, C., pg. 478), threats from criminal groups and bad

actors can be prevented. Having the power to monitor and identify potential threats is extremely important to helping organizations stay safe and not lose vital company data, in any form.

On the other hand, open-source intelligence gathered in many ways on the internet can be used to cause harm to companies and individuals. With this it is important to carry out regular IT Risk assessments performed through penetration testing as they "consist of system improvement recommendations along with evaluation reports… obtained from the collaboration analysis the OSINT concept, penetration testing methods, OWASP and ISO 31000 framework (Wiradarma, A. A. B. A., & Sasmita, G. M. A., pg. 17)." Putting these preventative measures in place to ensure a system is well protected is extremely important to protect against various threats to sensitive company information.

In addition, "information is always transparent, always open access, always readily available, and treated more as a community resource than an individual commodity (Glassman, M., & Kang, M. J., pg. 680)." This is very much the case in present day society as just about everyone has access to tons of information regarding many different topics right in their fingertips. Therefore, it is extremely important to watch and monitor what information, in various forms, is out on the web as public knowledge. This leaves some people skeptical as to who can view what information and for what purpose. In a study conducted by researchers at the Technical University of Darmstadt, "factors associated with the acceptance of…" open-source knowledge, "studied the use of surveillance technology to fight crime and terror, as well as to support people during human-made and natural disasters (Riebe, T., Biselli, T., Kaufhold, M.-A., & Reuter, C., pg. 488)." They found that more people were accepting of their data being utilized for purposes pertaining to these reasons. Privacy impacts will continue to raise concerns as time

progresses and there becomes even more uses for the plethora of information the internet and various software's provide.

Resources

Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior, 28(2), 673–682. https://doi.org/10.1016/j.chb.2011.11.014

Riebe, T., Biselli, T., Kaufhold, M.-A., & Reuter, C. (2023). Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey. Proceedings on Privacy Enhancing Technologies, 2023(1), 477–493. https://doi.org/10.56553/popets-2023-0028

Wiradarma, A. A. B. A., & Sasmita, G. M. A. (2019). IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*(12), 17–29. https://doi.org/10.5815/ijcnis.2019.12.03