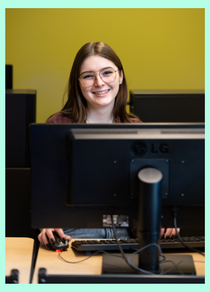
# ENRICHING HONEYPOT DATA USING CYBER THREAT INTELLIGENCE

Cybersecurity is a rapidly growing field that becomes more complex as time goes on. There are numerous aspects of security that branch out into their own equally complex fields. Many companies and organizations struggle to properly prepare for attacks against them, and fail to utilize threat intelligence or offensive security measures to mitigate these attacks.


## AUTHORS

Caitlin M. Allen and Adam Cunningham



## AFFILIATIONS

Presented to the faculty of the Information Technology & Sciences Academic Division at Champlain College for the Bachelor's of Science, Computer Networking & Cybersecurity and Bachelor's of Science, Computer & Digital Forensics

Under the Supervision of Dr. Ali Hadi and Dr. Elizabeth Allen-Pennebaker


## Introduction

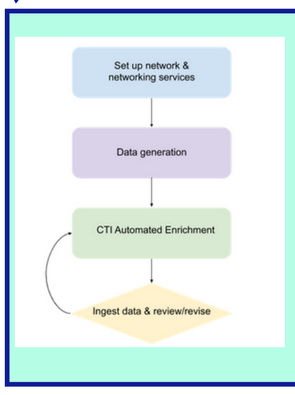
This project aims to take data gathered by honeypots to enrich reports that can be provided to cybersecurity experts to improve their security posture. While honeypots and threat intelligence are properly established in the field and have copious research behind their workings and capabilities, the knowledge around applying them to a readable format is limited. This research aims to bridge that gap between threat intelligence and security hardening. The project will be accomplished by creating a virtual network that emulates an enterprise network. Offensive security mechanisms will be installed on these machines in the appropriate sections to produce the results needed for enriching reports.

## Objective

The main objectives of this work can be summarized as the following:

- Setup, configuration, and deployment of honeypots on a virtual network
- Monitoring networks for intrusion detection and appropriately responding to these threats
- Collection of data to utilize in a report scheme that can be sent to cybersecurity experts to mitigate future threats

## Methodology

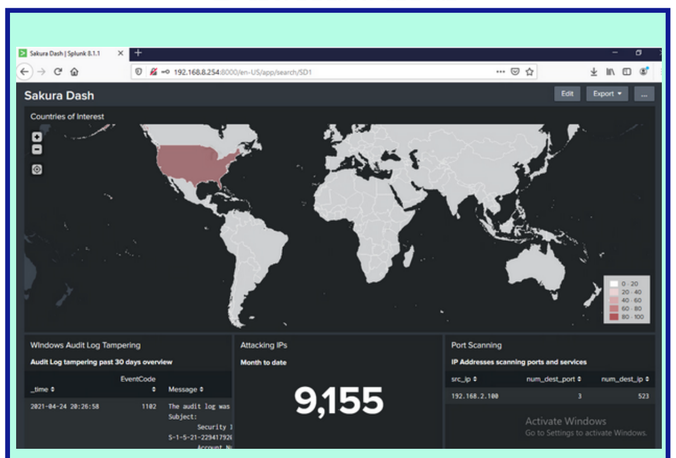


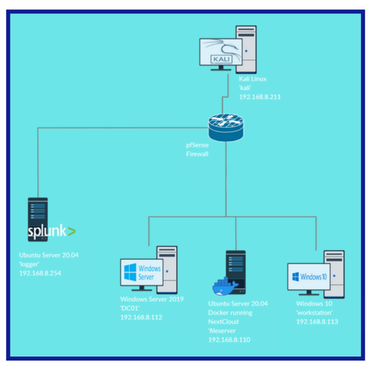

- Kali_Linux
- pfSense
- ubuntu-linux
- UbuntuSrv_20.04
- Windows-10
- Windows10_new
- WindowsServer

## Results

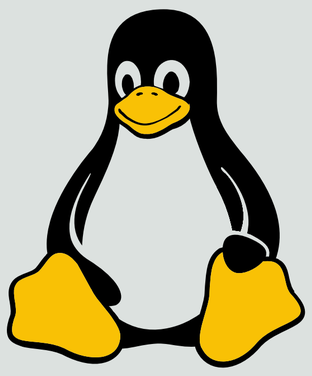
Our intelligence dashboard, Sakura Dash, shows malicious activity such as port scanning, distinct attacking IPs, countries of origin, Windows audit log tampering, and Linux shutdowns. We were able to see how many IP addresses were used to target the honeypot, where the IP addresses were originating from, as well as have an overview of what the attacker was doing in a broad overview. With this broad overview, we were able to investigate their interests in our web app and environment.

## Results Dashboard

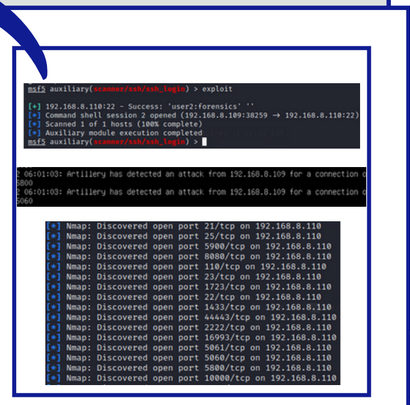



Network map of honeypot environment




SPL queries for dashboard searches




Screen captures from Kali Linux on the offensive side during emulated attacks and Artillery honeypot and IDS

## Conclusion

Overall, the project found that dashboards are the best way to visualize and present Threat Intelligence data to cybersecurity experts. Dashboards are a great way to visualize key metrics, and it makes the data easier to present both to cybersecurity experts, and those who may not have as much knowledge in the field. These dashboards are highly customizable, and can suit the security needs of any organization and display relevant data and fields.
The project also found that honeypots were a vital resource in detecting and identifying weak points in a network. They were a massive asset during the simulated attacks to find these threats, and can be a huge asset to an organization that wants to utilize these technologies. The honeypots were also helpful in preventing reconnaissance on the network, as the ports and IPs that were "opened" by the honeypots helped obscure finer details on the network.

## REFERENCES


ACE Team. (2018, December 11). Secure your Network by setting up a Honeypot - Loginsoft - Cybersecurity, Software Development, Offshore Services. Retrieved October 14, 2020, from https://www.loginsoft.com/blog/2018/11/16/secure-your-network-by-setting-up-a-honeypot/
Chen, J. (2020, July 01). Attacker's Tactics and Techniques in Unsecured Docker Daemons Revealed. Retrieved October 14, 2020, from https://unit42.paloaltonetworks.com/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/
Collier, K., Dilanian, K., & Winter, T. (2020, October 31). More hospitals hit by ransomware as feds warn about cyberattacks. Retrieved November 06, 2020, from https://www.nbcnews.com/tech/tech-news/more-hospitals-hit-ransomware-feds-warn-about-cyberattacks-n1245292
Curtis Simpson, O. (2020, October 02). Someone died because of ransomware: Time to give hospitals emergency security care. Retrieved December 10, 2020, from https://thehill.com/opinion/cybersecurity/519267-someone-died-because-of-ransomware-hospitals-emergency-security
Cyber Threat Intelligence 101. (n.d.). Retrieved October 25, 2020, from https://www.fireeye.com/mandiant/threat-intelligence/what-is-cyber-threat-intelligence.html
Department Of Defense. (n.d.). DoD COMPUTER NOTICE. Retrieved November 06, 2020, from https://www.dmdc.osd.mil/sevod/info/index.html
Dominguez, A. (2017, November 17). SANS Institute: Reading Room - Intrusion Detection. Retrieved October 27, 2020, from https://www.sans.org/reading-room/whitepapers/detection/paper/38165
Honeypots Study Guide. (n.d.). Retrieved November 07, 2020, from https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php
Kaspersky. (2020, September 10). What is a honeypot? Retrieved October 14, 2020, from https://usa.kaspersky.com/resource-center/threats/what-is-a-honeypot
Kaybay, M. E. (n.d.). Honeypots (4): Liability & Ethics. Retrieved November 7, 2020, from http://www.mekabay.com/nwss/206i--honeypots_(4).pdf
Kovacs, E. (2015, January 16). False Positive Alerts Cost Organizations $1.3 Million Per Year: Report. https://www.securityweek.com/false-positive-alerts-cost-organizations-13-million-year-report
Ng, C., & Green, A. (2020, March 30). Why A Honeypot Is Not A Comprehensive Security Solution. Retrieved November 06, 2020, from https://www.varonis.com/blog/why-a-honeypot-is-not-a-comprehensive-security-solution/
Oosthoek, K., & Doerr, C. (2020). Cyber Threat Intelligence: A Product Without a Process? International Journal of Intelligence and CounterIntelligence, 1-16. doi:10.1080/08850607.2020.1780062
Peter, E., & Schiller, T. (2008, April 15). A Practical Guide to Honeypot. Retrieved October 25, 2020, from https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/
Prizmant, D. (2020, July 15). Windows Server Containers Are Open. Retrieved October 14, 2020, from https://unit42.paloaltonetworks.com/windows-server-containers-vulnerabilities/
Radcliffe, J. (2007, March 16). CyberLaw 101: A primer on US laws related to honeypot deployments. Retrieved November 06, 2020, from https://www.sans.org/reading-room/whitepapers/legal/paper/1746
Sanders, C. (2020). Intrusion detection honeypots: Detection through deception. Oakwood, GA: Chris Sanders.
Sasson, A. (2020, May 31). Rootless Containers: The Next Trend in Container Security. Retrieved October 14, 2020, from https://unit42.paloaltonetworks.com/rootless-containers-the-next-trend-in-container-security/
Spitzner, L. (2003). Honeypots: Tracking hackers. Boston, MA: Addison-Wesley.
Symanovich, S. (2020, May 26). What is a honeypot? How it can lure cyberattackers. Retrieved October 14, 2020, from https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html
Threat Intelligence Definition. Why Threat Intelligence Is Important for Your Business and How to Evaluate a Threat Intelligence Program. (2019, October 02). Retrieved October 25, 2020, from https://usa.kaspersky.com/resource-center/definitions/threat-intelligence
Threat Intelligence: Everything You Need to Know. (2020, September 11). Retrieved October 25, 2020, from https://www.recordedfuture.com/threat-intelligence/
Wallen, J. (2019, October 02). How to quickly deploy a honeypot with Kali Linux. Retrieved October 14, 2020, from https://www.techrepublic.com/article/how-to-quickly-deploy-a-honeypot-with-kali-linux/
What is Cyber Threat Intelligence? [Beginner's Guide]. (2020, September 17). Retrieved October 25, 2020, from https://www.crowdstrike.com/epp-101/threat-intelligence/
What Is Threat Intelligence? Definition and Examples. (2019, May 14). Retrieved December 01, 2020, from https://www.recordedfuture.com/threat-intelligence-definition/
What is SIEM? A Complete Beginner's Guide - Varonis. (2020, June 15). Retrieved December 01, 2020, from https://www.varonis.com/blog/what-is-siem/
Zelivansky, A. (2020, September 10). The Challenge of Persistence in Containers and Serverless. Retrieved October 14, 2020, from https://unit42.paloaltonetworks.com/persistence-in-containers-and-serverless/