14 | OWASP Honeynet Experiment

Ethan Kortman, Hannah Fitzgerald, Michael Dedvukaj, Ashley Bekondo

Faculty Advisor: Dr. Tirthankar Ghosh

Department of Electrical and Computer Engineering and Computer Science

Abstract

Everything on the internet is susceptible to an attack, especially for an institution like the University of New Haven. The team will be conducting an experiment to implement the OWASP Honeynet framework onto the University CIT network. Doing this will allow the team to create a deception to the real network, drawing attackers away from the real network and putting them in a simulated copy of the real network. When the team is successful, we can present this to the University to show them how they can further their security posture as a whole in their environment of the network.

Objectives

1.Implement the honeynet to track attack patterns.

2.Successfully monitor traffic on the Honeynet.

3.Study attack patterns and methodology to understand how attackers move though the system.

4. Have a comprehensive list of recommendations for the university to take to improve the CIT network.

Problem Statement

While universities such as the University of New Haven have a substantial security infrastructure, there is always room for improvement. Our team is looking to find any vulnerabilities the network may have to recommend security improvements for the university through using a honeynet to mirror the University of New Haven networks.

Figure 1: OWASP Honeypot framework GitHub

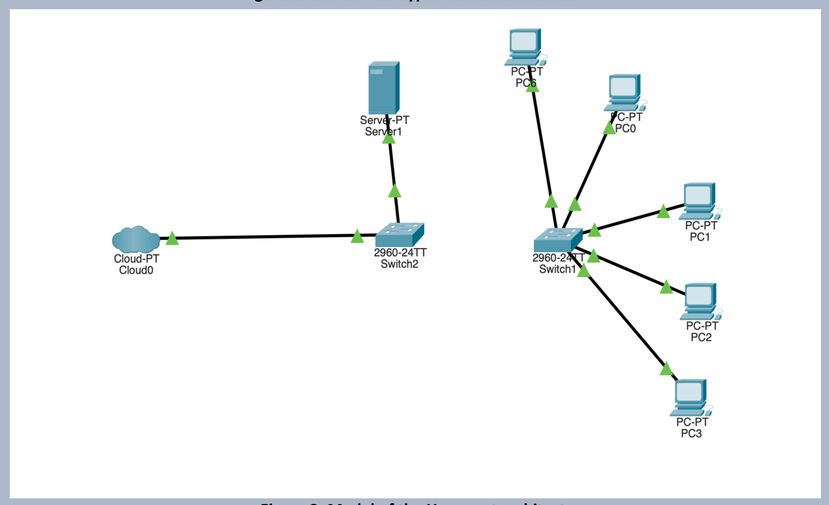

Figure 2: Model of the Honeynet architecture

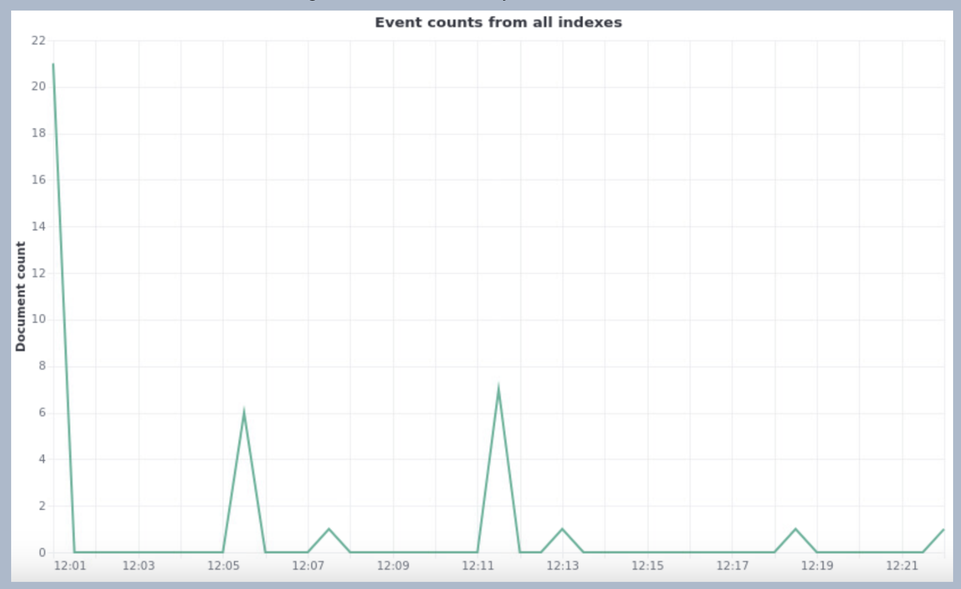

Figure 4: Visual from Kibana showing the attack occurring

Results

- Launched attack through CIT Network on the Database honeypot.
  - Changed user data
  - Encrypted data
  - Overwrote indices

- Network Restrictions through Firewall Usage
  - To change a password, require Multifactor Authentication
  - Restrict websites and other domains inside and outside of the network through NAT and Port Forwarding

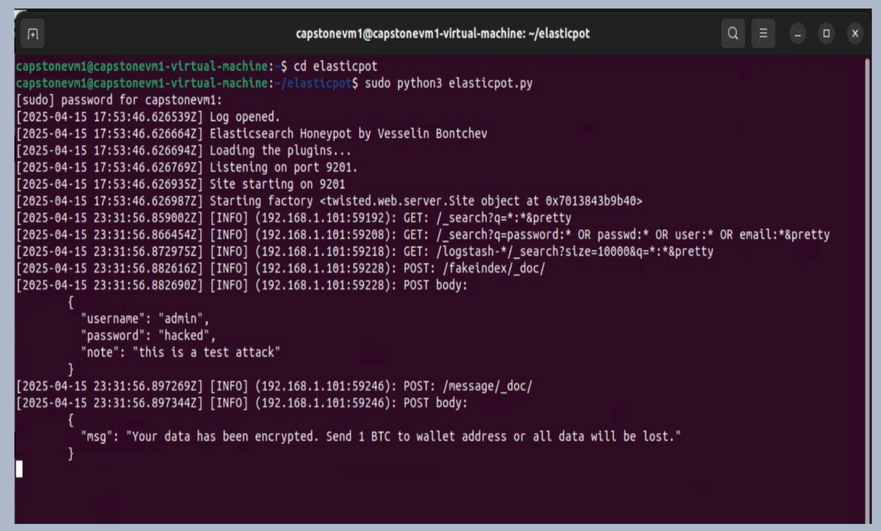

Figure 3: Attack launched on database honeypot

Future Research

- Furthering this project would include:
  - Implementing more honeypots
    - Webservice
    - SSH
    - DNS

  - Continue testing Elasticpot and OWASP to further strength our university's network security posture

  - Presenting the data to the University in order to recommend the best security changes possible

Acknowledgements

Faculty Advisor: Dr. Tirthankar Ghosh