A HoneyNet Environment for Analyzing Malicious Actors

2018 Marist College / IBM Joint Study
Students Daniel N. Gisolfi, Michael Gutierrez, Tyler V. Rimaldi
Faculty Robert Cannnistra, Casimer DeCusatis , Matthew Johnson, Alan G. Labouseur
IBM Greg Lacey

What

A honeypot is a web application or other resource that is deceptively constructed to log the actions of its users, most (but not all) of whom can be assumed to be malicious actors. A honeynet is a network of interconnected honeypots that allows vast amounts of data to be collected for analysis. This poster describes our honeynet and shows some insights we gained by analyzing attack data we gathered from it.

Why

We came to develop our (high interaction) honeynet through the evolution of our cyber security research that began by using graph analytics to examine data collected from individual (low interaction) SSH and SDN honeypots. In combining these honeypots, we developed a high interaction honeynet to collect vast amounts of attack data. We hope to uncover attackers' strategies, motives, and investments, and thus provide insight on how to prevent or mitigate similar attacks.

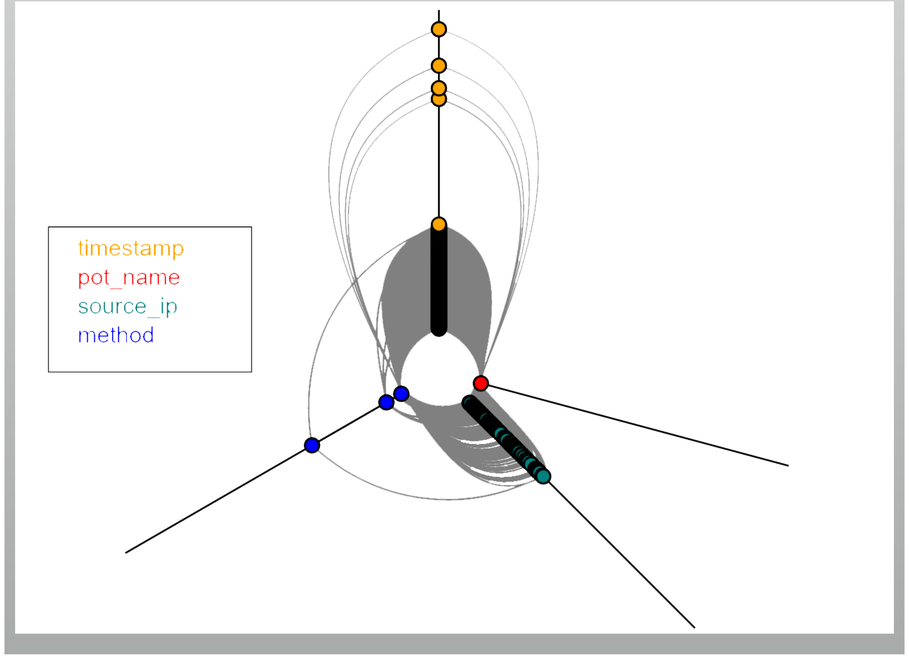
This work is sponsored in part by NSF Grant Award 1541384 — CC*DNI Integration: Application Aware Software-Defined Networks for Secure Cloud Services

Preliminary Analysis

We have found, even at this early stage, multiple types of recurring attacks that include attempts to kill a PHP5 hash function and CGI (Common Gateway Interface) attempts to access Apache files.

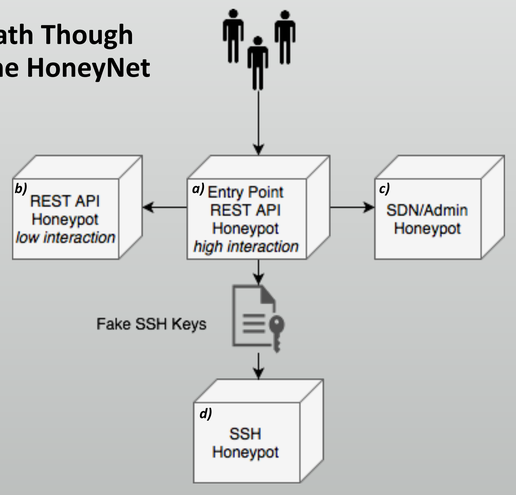
PHP
- GET phpeval=die(md5('PHP'));
- GET http://xxx.yyy.210.12/yup.php
- GET http://xxx.yyy.210.12/echo.php
- GET /phpMyAdmin/index.php

CGI
- GET /login.cgi
- GET /cgi-bin/ luci/;stok=redacted/expert/ maintenance/diagnostic/ nslookup



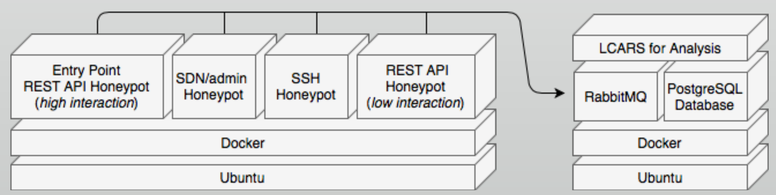
HoneyNet Construction

Path Though the HoneyNet



a) Java and NanoHTTPD, REST API with redirect commands linking to either *b* or *c*. Contains fake SSH keys leading to *d.*
b) Java and NanoHTTPD, REST API that takes any HTTP request and responds with `<h1>404 Not Found</h1>`.
c) Python and Flask, SDN/System Admin honeypot that prompts attackers for credentials. If accessed, lists contents pulled fromPostgreSQL.
d) C and Perl, SSH honeypot; terminating point.

Deployment and Activity Tracking



Deployment
- Hosted at Marist College on IBM cluster
- Honeynet contents are scattered across multiple TCP ports on a single network with a public IP address.
- Each honeypot resides in their own Docker container running in a standalone, dedicated Unix environment (Ubuntu).
- Honeypot VM ports mappedto Docker sub-network ports on the host machines.
- RabbitMQ is used to collect logs, which are visualized in our **L**ightweight **C**loud **A**pplication for **R**eal-time **S**ecurity (LCARS) tool.

Tracked Data
- Timestamp
- HoneyPot
- Host IP
- Host PID
- HPID
- Method
- Requested_Text
- Source IP
- Source Port
- User Agent
- Post Text
- Source Country
- Country Code

This work was influenced by The Honeynet Project, an international 501(c)(3) non-profit security research organization, and by the book, *Introduction to Cyberdeception* by Neil C. Rowe and Julian Rrushi. We would like to thank our fellow students in the Marist/IBM Joint Study as well as the faculty and staff for their encouragement and contributions.