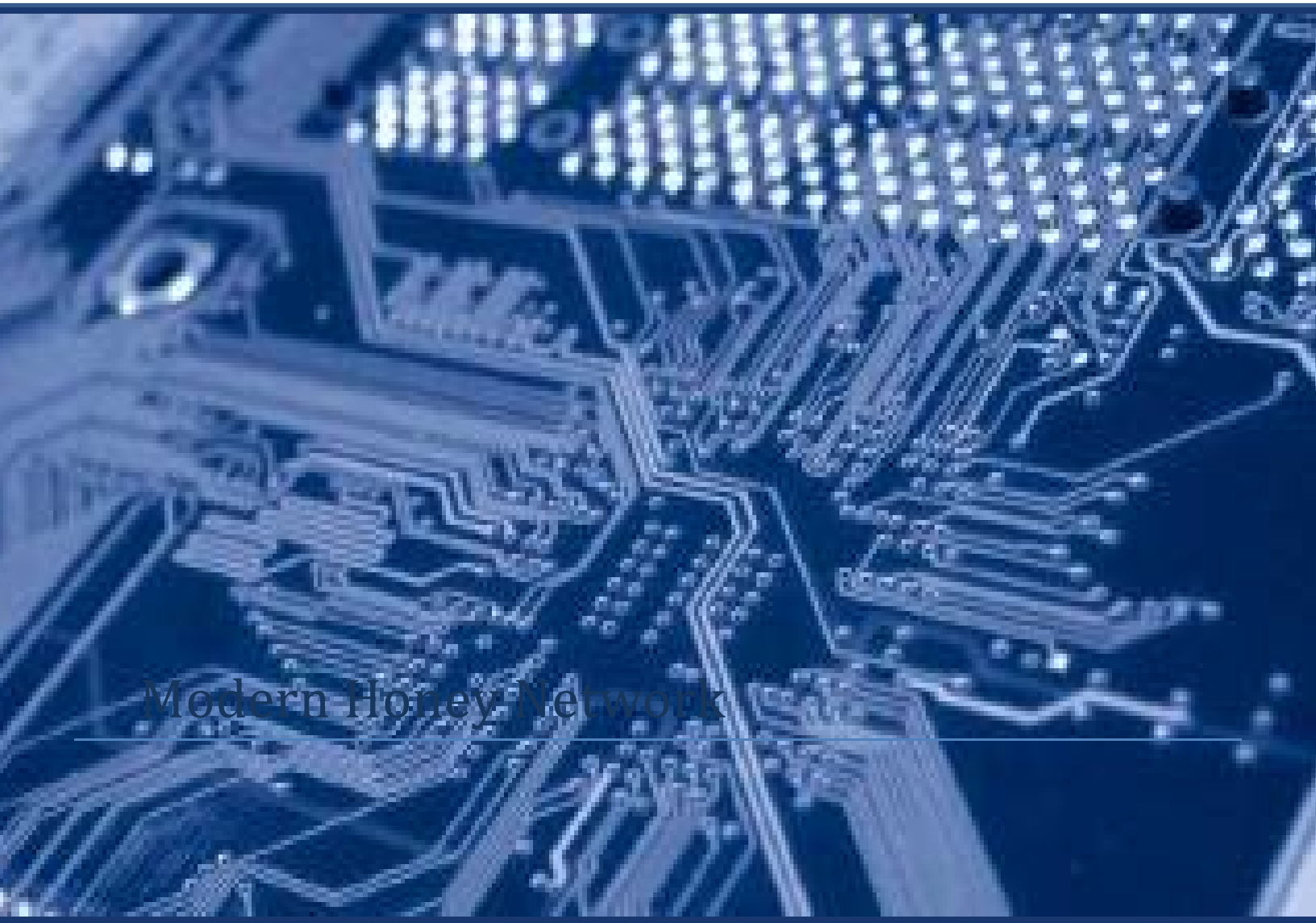
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation



Modern Honey Network

175 Lakeside Ave, Room 300A
Phone: (802)865-5744
Fax: (802)865-6446
http://www.lcdi.champlain.edu

11/16/2015

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Table of Contents

Introduction

This project assessed the Raspberry Pi, a low cost, credit card-sized computer that can connect to a standard display and utilize keyboard/mouse input, and the viability of it redefining how cyber security specialists view honeypots. Traditionally, a honeypot is an isolated server within a network that is purposely accessible to attackers in order to detect, document, and archive various types of malware, spam, and intrusion methods. This project explored a Modern Honey Network (MHN), a honeypot network powered by multiple Raspberry Pi machines in an attempt to create a simpler and more cost-effective honeypot framework. The project also used a honeypot program called Dionaea to analyze the Raspberry Pi's sensors within the MHN and explore their flexibility.

Background:

The Pi Cyber project was undertaken to both immerse new FOR-190 interns into work at the LCDI as quickly as possible and provide the investigation center with a new inroad for research into honeypots. Our initial research suggested that honeypots have not yet become a widespread asset in company networks. According to a blog post by Jason Trost, Vice President of ThreatStream, "honeypots have not received wide adoption as an enterprise defense largely because the deployment and management has been a complicated process reserved for security companies and computer researchers" (Trost). Over the duration of this project, the Pi Cyber team hopes to mitigate these fundamental drawbacks by designing an alternative approach to the honeypot network. We believe that utilizing a system of Raspberry Pi machines aggregated by ThreatStream's Modern Honey Network (MHN) software will create the foundation for a honeypot with a significantly lower cost and operational footprint than conventional methodologies and simplify deployment procedures by a wide margin.

Purpose and Scope:

The LCDI undertakes research projects in order to support the advancing fields of digital forensic investigation and cyber security, along with the companies, firms and departments that utilize them. Honeypots are a great tool to reinforce system security by detecting intrusion attempts and network scans. This project aims to generate data that will aid in assessing the viability of the Raspberry Pi/MHN suite as an alternative to traditional honeypot systems and assess its flexibility using Dionaea.

Research Questions:

1. What are the discernible advantages of Raspberry Pi honeypots?
2. What is required, if anything, to turn a disjoint set of Raspberry Pi honeypot sensors into a fully-fledged honeypot network?
3. Is there a certain volume of traffic / type of traffic that can easily or quickly overwhelm the Raspberry Pi setup?

Terminology:

Honeypot – a system that's put on a network so it can be probed and attacked; any interaction with a honeypot, such as a probe or scan, is by definition suspicious

Dionaea – honeypot sensor software which spoofs services on ports and records attacks on the spoofed services

Modern Honey Network – honeypot management and data aggregate system

Raspberry Pi – low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse (Will often be referred to as RasPi thorough this report)

Raspbian – fork of Debian (GNU/Linux distribution) optimized for the Raspberry Pi hardware.

Methodology and Methods

In order to create a subnet of Raspberry Pi devices isolated from the LCDI network for use as honeypot sensors, a separate Dynamic Host Configuration Protocol (DHCP) server was necessary to keep the machines from contacting any device outside of the MHN subnet. The team requisitioned a designated project server that would host the MHN as well as the new DCHP, and the Raspberry Pis were arranged to receive IP addresses. At this time, the Python-based MHN installer failed to execute correctly during the initial setup because it required that a MongoDB (a commercial database server) client be present on the machine. In order to be compatible with MongoDB, the server's operating system was downgraded from Ubuntu 15.04 to 14.04 LTS. As a result of these modifications and additions, MHN was installed on the project server with no further error.

Early in the process, the team agreed that the offline DHCP server should be abandoned and instead the honeypot be placed in a subnet within the LCDI network. This decision came from the realization that this separate server would be unable to establish connections to aptitude package servers required to update MHN through its Dionaea deployment script. However, when the new subnet was created, we saw that the Raspberry Pis could be accessed by multiple IP addresses; some were within the subnet mask, while others were aligned to the main LCDI network.

Equipment Used

Name	Quantity	Purpose
Project Server	One (1)	Host the Modern Honey Network
Raspberry Pis with 8GB Micro SD Cards, USB Wi-Fi adapter and 5v Micro USB power supplies	Five (5)	Dionaea Sensor
Network Switch	One (1)	Creating the network between the project server and the Pis

A Raspberry Pi is a credit-card sized (approx. 3 ½" x 2" x 1"), ARM-core based miniature computer. Although it boasts a lower clock speed, less memory, and far fewer options for general peripherals, its small size and comparatively low cost (with the kit we used costing approximately $100 for the Pi + peripherals, case, and

assorted odds and ends) makes it a prime choice for utilization in distributed computing/networking solutions, such as honeypot networks.

Table 1: Devices

Name	Purpose
Project Server	MHN host
Raspberry Pi CyberPi01	Dionaea Sensor
Raspberry Pi CyberPi02	Dionaea Sensor
Raspberry Pi CyberPi03	Dionaea Sensor
Raspberry Pi CyberPi04	Dionaea Sensor
Raspberry Pi CyberPi05	Dionaea Sensor

Analysis

This project was created to test the viability of a honeypot network using Raspberry Pis in conjunction with the Modern Honey Network software. We expected the Raspberry Pis to be an effective sensor for a honeypot network based on their low cost and minimal digital footprint. However, Dionaea seemed limited and lacked flexibility due to being a low interaction honeypot by design.

Our initial sweeps of the subnet somewhat validated our predictions. Although each port accessed generated an individual entry in the MHN logs, the information it contained was rudimentary, consisting of a basic description of the type of access, the IP address of the sensor, and the IP address of the accessor. Further inquiry proved that attempting to access a sensor's File Transfer Protocol (FTP) process returned a falsified sandbox on which an attacker's activities, such as file uploads and downloads, could be logged. Further areas of experimentation which were not directly approached over the course of this project, due to time and complexity constraints, include interactions with Samba (a software suite that provides compatibility between Windows and Linux clients) and Structured Query Language (SQL) server access.

Upon examining the MHN logs of sensors that possessed multiple IP addresses, we saw that LCDI equipment (such as 192.168.10.4, determined through an NMAP scan to be a "secret sweeper" for the LCDI) had communicated with the devices and collected data regarding the type of access attempts made.

Data Collection

Table 2: Sample data from MHN logs, from device cyberpi02

Date	Destination Port	Protocol
2015-10-21 13:57:41	445	smbd
2015-10-21 13:56:50	445	smbd
2015-10-21 13:55:59	445	smbd
2015-10-21 13:55:59	42	mirrord
2015-10-21 13:55:59	38349	mirrorc
2015-10-21 13:55:59	1433	mssqld

Results

Raspberry Pis present themselves as viable alternatives to consumer grade honeypot sensors when paired with competent aggregation and deployment software like the Modern Honey Network. They were easy to deploy, largely mitigated the attached costs, and carried small footprints. Deployments with Dionaea, although initially appearing limited, offered great flexibility through multiple port selections such as SQL, FTP, SAMBA shares, and HTTP.

1. **What are the discernible advantages of Raspberry Pi honeypots?**
   Raspberry Pi computers have the advantage of being relatively inexpensive and low profile devices, with essential functionality still intact and with fair performance for the size of each device, making them a feasible asset as honeypot sensors.
2. **What is required, if anything, to turn a disjoint set of Raspberry Pi honeypot sensors into a fully-fledged honeypot network?**
   Each individual sensor requires the installation of honeypot software along with basic manual configuration to attach it to the network. In addition, a server of some kind is necessary in order to aggregate the data and simplify deployment by utilizing the Modern Honey Network software.
3. **Is there a certain volume of traffic / type of traffic that can easily or quickly overwhelm the Raspberry Pi setup?**
   A concentrated, well-distributed surge of traffic has the potential to overwhelm a collection of Raspberry Pis, but this much is true for any network of computers.

Conclusion

Honeypot frameworks utilizing Raspberry Pis as sensors are far easier to deploy, have a much smaller footprint, and are cheaper than traditional honeypots, while retaining flexibility and ease of information analysis. The team has concluded that with the proper load balance over a network of five to ten Raspberry Pi machines, it would be infeasible (however, not impossible) to overload the sensors with traffic. However, one present issue is that scanning applications like Nmap can identify the sensors as a honeypot. Since honeypots are intended to be shown as little more than a normal asset within a network, this lack of invisibility may alert attackers. Furthermore, Dionaea, which is classified as “low interaction honeypot” software, was shown to be inflexible and limited in its uses, primarily restricted to recording the IP of port access attempts, which does not allow for direct action to be taken or a motive to be established.

Further Work

We would like to conduct further research into MHN/Honeypots to further explore how we can improve our system and work with different types of honeypots, including those with higher levels of interaction. Notable alternatives include Kippo (an SSH honeypot used to detect and monitor brute force attacks), Conpot (which disguises itself as an Industrial Control System to draw attackers with malicious intent), and Snort (another Intrusion Detection System). Each of these solutions can be integrated within the Modern Honey Network system that was used in this project to manage the Dionaea software deployed over a number of Raspberry Pi devices. On the other side of security, the Raspberry Pi can be used in different methods of hacking into a system including cloud sync intrusion, man in the middle attacks (where the device interposes in

a two-way communication), and Near-Frequency Communication/Radio Frequency Identification signal interception. The portability of the Raspberry Pi makes it a great option for penetration testing, which would require a user to put the Pi on another network and have it act as a packet sniffer on the network until the owner retrieves it again.

Work Cited

- Trost, Jason. "Blog." Modern Honey Network. Web. 9 Nov. 2015.
- Evans, Loras. "Intrusion Detection FAQ: What Is a Honeypot?" SANS. Web. 14 Sep. 2015.
- "Threatstream/mhn." GitHub. Web. 14 Sept. 2015.