**University of the Incarnate Word**

**Raspberry Pi-based honeypot(DShield)**

**Abdulrahman Alqarni**

**Course Name: Cyber Systems and Components Instructor: Dr. Gonzalo D. Parra**

**Date: 2/2/2024**

## EXECUTIVE SUMMARY

The aim of this project is to set up a Raspberry Pi-based honeypot using the DShield Honeypot software to gather information about potential cyber threats and attacks. This report outlines the steps involved in setting up and configuring the Raspberry Pi honeypot.

Project Milestones:

1. **Setup and Configuration:**
   * Install Raspberry Pi OS and required software.
   * Clone DShield Honeypot repository and configure.
2. **Testing and Validation:**
   * Ensure proper network connectivity.
   * Confirm honeypot captures and logs threats accurately.
3. **Integration and Optimization:**
   * Fine-tune honeypot settings.
   * Test against simulated attacks.
   * Optimize Raspberry Pi resources.
4. **Documentation and Reporting:**
   * Document setup and configuration.
   * Create technical report.
   * Prepare a project summary presentation.

Professional Accomplishments:

1. **Successful Setup and Configuration:**
   * Installed and configured Raspberry Pi OS and DShield Honeypot.
2. **Effective Testing and Validation:**
   * Validated honeypot's ability to capture and log threats.
3. **Efficient Integration and Optimization:**
   * Fine-tuned honeypot settings for optimal performance.
   * Tested resilience against simulated attacks.
   * Optimized Raspberry Pi to my own case.
4. **Comprehensive Documentation and Reporting:**
   * Documented setup and configuration process.
   * Created a concise technical report.

## PROJECT SCHEDULE MANAGEMENT

Link to Trello= https://trello.com/invite/b/DWWNPsvF/ATTI46d04066f14b07d0336803433ab02b1112AE2431/me

Link to github repository=

https://github.com/alqarni360/Raspberry-Pi-based-honeypot.git

### Download Raspberry Pi Image Loader

First we have to download the Raspberry Pi Image Loader software from the official Raspberry Pi on their official website.

<https://www.raspberrypi.com/software/>

A screenshot of a computer

Description automatically generated

### Prepare SD Card:

Insert the SD card into the computer using a memory card reader.

### Load Operating System:

Open the Raspberry Pi Image Loader software and use it to load the operating system onto the SD card (referred to as "Bake Your Pi").

### Set up Raspberry Pi:

Insert the SD card into the Raspberry Pi and power on the device.

### Update Raspberry Pi:

I execute this command “sudo full-upgrade” to update the Raspberry also Pi's software packages.

Reboot Raspberry Pi: Reboot the Raspberry Pi using the command sudo reboot.

Install Git: Install Git version control system using the command sudo apt-get -y install git.

A screen shot of a computer

Description automatically generated

### Download DShield Honeypot:

Installation of DShield Honeypot was conducted by obtaining the source code from the official GitHub repository maintained by DShield-ISC. The installation process was initiated following the instructions provided on the GitHub repository. Additional guidance and insights on the installation procedure are available on their github site. Screenshots illustrating the installation steps have been appended to this document for reference.

GitHub, <https://github.com/DShield-ISC/dshield>

After installation Change Directories and I navigate to the dshield/bin/ directory using the command cd dshield/bin/.

And executed the installation script using the command sudo ./install.sh

### DShield setup:

After running the installation script, I encounter a page with the message: "You are about to turn this Raspberry Pi." Please read this message carefully.

A computer screen with a message

Description automatically generated

Continue selecting "Next" until you reach the page where you can set the option to automatic.

When you reach this page, it prompts you to obtain an API key, which I can acquire after signing up on the DShield website. Follow my next steps.

A computer screen with a blue screen

Description automatically generated

I Visited the DShield website to create an account and obtain my API key. You can create an account by

Create an account on the following link : https://isc.sans.edu/register.html?ts

A screenshot of a computer

Description automatically generated

After signing up, you will need to confirm your email address by visiting the link that will be sent to your email inbox.

After logging to your account the API key should be on the home page :

A screenshot of a computer

Description automatically generated

Now, return to the previous page I havee entered my API key and email address into the designated fields as shown in the image.

A computer screen with a blue screen

Description automatically generated

A computer screen shot of a computer

Description automatically generated

Next, I will set the credentials that will be used to access the administrative privileges and receive comprehensive reports of your honeypot via email.

A computer screen shot of a computer

Description automatically generated

After completing the previous steps, with no further changes required, the next step was to reboot the system. $sudo reboot.

### Scan against my honeypot using nmap:

I used a different machine to run the scan on my honeypot using Nmap with the following command:

$nmap -Pn -A 192.168.1.117

A screenshot of a computer

Description automatically generated

The scan came back as expected, revealing numerous vulnerable services.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

### Honeypot Auto Report

Any attack technique used against the honeypot will be saved as a report on the DShield website in my dashboard account. These reports are updated regularly every 30 minutes.

A screenshot of a computer

Description automatically generated

### Conclusion:

I have successfully constructed a Raspberry Pi-based honeypot utilizing the DShield Honeypot software. This project embodies a profound exploration into the realm of cybersecurity, offering a practical understanding of threat detection and mitigation.

5/7/2024

University of The Incarnate Word Attention: Dr. Gonzalo. D. Parra 4301 Broadway

San Antonio, TX 78209 Dear Dr. Parra:

With this letter, the team Alqarni transmits the following items associated with the **CIS 3353 Final Project**.

**SCOPE OF WORK (dated 5/7/2024): “Raspberry Pi-based honeypot**

**”**

Please share these with your team as appropriate. If you have any questions, please contact

My phone at (726) 214-0453 or by email at alqarnifx360@gmail.com.

Kindest regards,

Team Lead

Student of Cyber Security Systems at the University of the Incarnate Word