

User's Manual

Network Server Honeypot



October 6, 2021

Group 8

|  |  |  |
| --- | --- | --- |
| **Release No.** | **Date** | **Revision Description** |
| Rev. 0 | 6/10/2022 | Initial Draft |
| Rev. 1 | 24/10/2022 | Final Revision |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
|  | **User’s Manual**  **Authorization Memorandum** |

I have carefully assessed the User’s Manual for Group 8’s Network Server Honeypot. This document is accordance with the specifications and necessities of Bad Security Inc.

We fully accept the initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NAME: Jose Protacio DATE

Team Leader

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NAME: Christopher Hollingsworth DATE

Planning Manager

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NAME: Joseph Leong Yiu Joe DATE

Quality Control Manager

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NAME: Karima Bassyouni DATE

Development Manager

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NAME: Ryan Mudford DATE

Client Liaison

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NAME: Malimage Manthi Athulya Fernando DATE

Support Manager

**USER'S MANUAL**

**TABLE OF CONTENTS**

Page #

A. GENERAL INFORMATION A-1

1.1 Purpose A-1

1.2 Scope A-1

1.3 System Summary A-1

1.3.1 What it is and what it does A-1

1.4 Key Features A-1

1.4.1 Logging A-1

1.4.2 IP Ban A-1

B. SYSTEM SET-UP B-1

2.1 First-time users B-1

2.2 Installing the Docker images B-1

2.2.1 How to install using GitHub Repository B-1

2.3 Installing the Dockerfiles and Bash Scripts B-1

2.3.1 How to install using GitHub Repository B-1

2.3.2 How to set up B-1

C. USING THE SYSTEM C-1

3.1 Logs C-1

3.1.1 Viewing Logs C-1

3.1.2 Filtering Logs C-1

3.2 IP Ban C-1

3.2.1 Viewing active connections C-1

3.2.2 Banning specific connections C-1

D. Accounts and other useful information D-1

4.1 Admin Accounts D-1

4.1.1 Vulnerable Web Server D-1

4.1.2 Vulnerable System Server D-1

4.1.3 Secure Logging Server D-1

**1.0 GENERAL INFORMATION**

# GENERAL INFORMATION

## 1.1 Purpose

## This manual was created to guide Bad Security Inc employees in properly deploying the system as well as other accompanying tools on their systems. It is also to guide users with the proper do’s and don'ts along with the provision of knowledge on key features of the system.

## 1.2 Scope

This user manual will cover basic fields in understanding the system’s functions. The fields that will cover in this user manual are listed below:

* Key features of the application.
* Necessary software needed to be downloaded for first-time users.
* Step-by-step instructions in operating the system.

This user manual would not cover the section below:

* FAQ (Frequently Asked Questions).
* Fixing any errors or bugs in the code
* Alteration, updates, or deletion of functions

**Note:** This user manual is written with the assumption that the user has working knowledge with regards to networking, Linux, Docker, and the use of the command line interface.

## 1.3 System Summary

### 1.3.1 What it is and what it does

This system is a series of servers encompassing a vulnerable web server, vulnerable system server and a secure logging server. It aims to provide Bad Security Inc with information regarding potential attackers and an avenue to act against them.

## 1.4 Key Features

### 1.4.1 Logging

**1.4.1.1** **Viewing logs**

This feature is used to view all packet and command logs from both the web and system server. It is done through the logging server using the provided web portal.

**1.4.1.2** **Filtering logs**

This feature allows users to filter logs based on certain fields such as IP or type.

### 1.4.2 IP Ban

**1.4.2.1 Viewing active connections**

This feature allows users to view active connections to the server using the provided web portal.

**1.4.2.2 Banning specific IP Addresses**

This feature allows users to ban specific connections using the provided web portal.

**2.0 SYSTEM SET-UP**

# SYSTEM SET-UP

## 2.1 First-time Users

The initial files of the servers would need to be downloaded onto the user’s computer. This system requires the use of Dockerfiles and Bash Scripts.

## 2.2 Installing the Docker Images

**Note:** The system would be requiring the user to have Docker as a service on their Linux environment. This step must be done before subsequent steps below can be completed.

**2.2.1 How to install using the GitHub Repository:**

Provided below is the link to the repository containing the necessary information and links

GitHub Repository: <https://github.com/JoseProtski/SEP-G8-Honeypots>

## 2.3 Installing the Dockerfiles and Bash Scripts

**2.3.1 How to install using the GitHub Repository:**

Provided below is the link to the repository containing the necessary information and links

GitHub Repository: <https://github.com/JoseProtski/SEP-G8-Honeypots>

**2.3.2 How to set up the files:**

The following instructions are regarding the Dockerfiles. These need to be done for all three servers.

**Note: Bold are commands to be used exactly**

**Note:** *Italics need to be replaced by the user*

Set up the files and the folders in the root/home directory

* E.g. SecureLoggingServer(Folder)/Dockerfile(File)

**Note:** This will be used to build the image later

**Note:** Dockerfile has to be called “Dockerfile”

* Build the image
  1. **docker build . -t** *anynewtagname* **-f** *foldername***/Dockerfile**

The following instructions are regarding the bas scripts. This needs to be done for all three servers and the mysql\_startup.sh within the Secure Logging Server.

**Note:** mysql\_startup.sh needs to be created and committed first before creating the bash script for the Secure Logging Server

Create script using provided script

1. **Touch** *scriptname*.**sh**
2. **Nano** *scriptname****.sh***
3. Copy and paste the appropriate script
   1. Change the ID to the new one based off the Build
4. Exit and save
5. Set permissions for script to run
   1. **Chmod u+x** *scriptname***.sh**
6. To run
   1. **./***scriptname***.sh**

**3.0 USING THE SYSTEM**

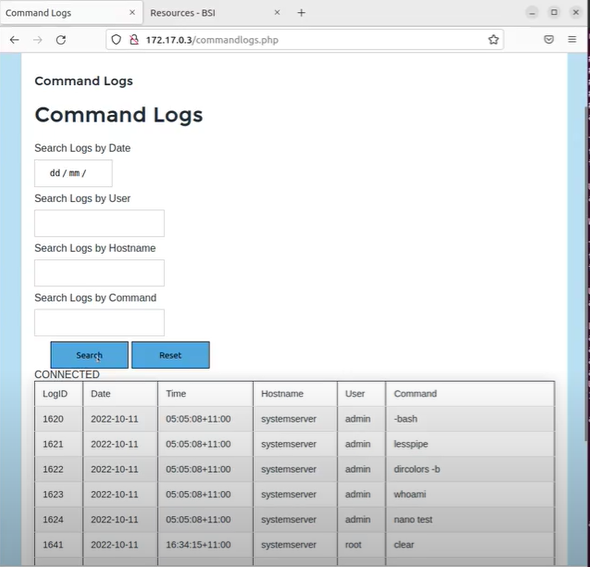
# USING THE SYSTEM

## 3.1 Logs

Note: The following portions assume all services are running and functioning within normal conditions

**3.1.1** **Viewing Logs**

Use the web portal provided – 172.17.0.3/commandlogs.php



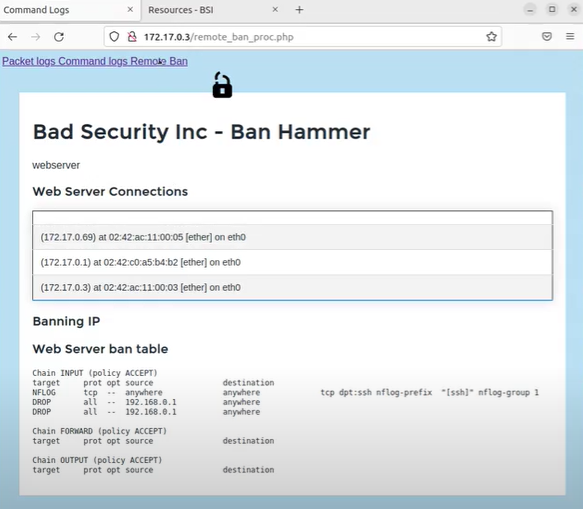
**3.1.2** **Filter Logs**

Use the search filters provided

## 3.2 IP Ban

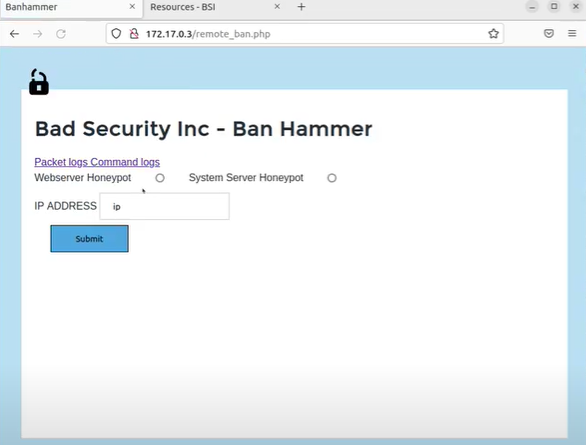
**3.2.1** **Viewing active connections**

Navigate to the IP Ban page - 172.17.0.3/remote\_ban.php



**3.2.2** **Banning Specific connections**

Type the ip address of the IP to ban in the field and submit

****

**4.0 ACCOUNT AND OTHER USEFUL INFORMATION**

# Account information

## 4.1 Server Accounts

### 4.1.1 Vulnerable Web Server Accounts

* **Real Admin Account** 
  + **Username:** Administrator
  + **Password:** password
* **Fake Admin Account**
  + **Username:** admin
  + **Password:** password

### 4.1.2 Vulnerable System Server Accounts

* **Real Admin Account** 
  + **Username:** Administrator
  + **Password:** password
* **Fake Admin Account**
  + **Username:** admin
  + **Password:** password

### 4.1.3 Secure Logging Server Accounts

* **MYSQL Root Account**
  + **Username:** root
  + **Password:** password
* **MYSQL User Account**
  + **Username:** admin
  + **Password:** badsecurityinc

### 4.1.4 Vulnerable Website

* **Account**
  + **Username:** allan
  + **Password:** badsecurity