Project Script File: Enhancing Network Security with Snort IDS and Honeypot Integration

Note: This script provides a is only possible to run in Linux Type of Operating System.

I. Honeypot Setup (Pentbox)

1. **Install Pentbox:**

- Download Pentbox from a reliable source.
- Extract the Pentbox archive.
- Navigate to the Pentbox directory.
- Make the Pentbox executable.

```
# Example (adapt to your system)
wget https://github.com/some/pentbox.tar.gz # Replace with
actual download link
tar -xvf pentbox.tar.gz
cd pentbox
chmod +x pentbox.rb
```

2. **Configure Honeypot:**

- Run Pentbox.
- Choose "Honeypot" from the main menu.
- Select a configuration mode:
  - **Fast Auto Configuration:** Quick setup with default settings.
  - **Manual Configuration:** Customize settings (port, message, logging, etc.).
- If using Manual Configuration:
  - Specify the listening port (e.g., 80 for HTTP).
  - Enter a custom message to display to attackers.
  - Enable/disable logging.
  - Enable/disable sound alerts.

```
Example (Manual Configuration)
./pentbox.rb
# ... (follow the Pentbox menu prompts)
```

3. **Isolate Honeypot:**

- Ensure the honeypot is deployed on an isolated network segment. This is crucial to prevent attackers from gaining access to your production network.
- Use a separate virtual machine, VLAN, or physical network.
- Configure firewall rules to restrict traffic to/from the honeypot.

```
# Example (iptables - adapt to your firewall)
iptables -A FORWARD -i eth0 -s 192.168.100.2 -j DROP  #
Block forward from honeypot
iptables -A FORWARD -i eth0 -d 192.168.100.2 -j DROP  #
Block forward to honeypot
```

II. Snort IDS Setup

1. **Install Snort:**

- Install Snort and its dependencies. The exact steps vary depending on your operating system (Linux, Windows, etc.).

```
# Example (Ubuntu)
sudo apt update
sudo apt install snort
```

2. **Configure Snort:**

- Configure Snort to capture traffic on the network interface connected to the honeypot network segment.
- Edit the Snort configuration file (e.g., /etc/snort/snort.conf).
- Define the network variables (HOME_NET, etc.).
- Specify the network interface to monitor.
- Include the necessary Snort rules.

```
# Example (snort.conf)
ipvar HOME_NET 192.168.100.0/24  # Honeypot network...
dev eth1  # Interface connected to honeypot network
include $RULE_PATH/snort.rules # Include rule file.
```

3. **Write Snort Rules:**
   - Create Snort rules to detect traffic to/from the honeypot. These rules will generate alerts when attackers interact with the honeypot.
   - Create a new Snort rule file (e.g., /etc/snort/rules/honeypot.rules).
   - Write rules to detect specific actions, such as TCP connections to the honeypot's listening port.
     - Use the Snort rule language.
   - Include the new rule file in the main Snort configuration file (snort.conf).

```
# Example (honeypot.rules)
alert tcp any any -> $HOME_NET 80 (msg:"ATTACK: Attempted
connection to honeypot"; sid:1000001; rev:1;)
```

4. **Start Snort:**
   - Start Snort in IDS mode, specifying the configuration file and the network interface.

```
snort -c /etc/snort/snort.conf -i eth1 -A console
```

III. Integration and Testing

1. **Test the Integration:**
   - From a separate system (the attacker's system), attempt to connect to the honeypot (e.g., using telnet, nmap, or a web browser).
   - Verify that the honeypot responds as expected (displays the custom message, logs the connection).
   - Verify that Snort generates an alert when the connection attempt occurs.
   - Check the Snort alert output (console, log file) for the alert message.
2. **Monitor and Analyze:**
   - Continuously monitor Snort alerts and honeypot logs.
   - Analyze the attacker's activity to gather information about their TTPs.
   - Use the collected information to improve your overall security posture.