HoneyTrap: Lightweight Honeypot Setup on Kali Linux

Step 1: Setting Up HoneyTrap

1. **Install Dependencies**

   sudo apt update && sudo apt install -y git python3 python3-pip

2. **Clone HoneyTrap Repository**

git clone https://github.com/honeytrap/honeytrap.git

cd honeytrap

3. **Install HoneyTrap**

make install

4. **Verify Installation**

honeytrap --version

Step 2: Configuring HoneyTrap

1. **Modify Configuration File** (/etc/honeytrap/honeytrap.conf)
   Example basic config:

yaml

[listener]

type = "tcp"

listen = ":2222"

[services.ssh]

enabled = true

logdir = "/var/log/honeytrap"

2. **Run HoneyTrap**

sudo honeytrap -c /etc/honeytrap/honeytrap.conf

3. **Check Logs**

cat /var/log/honeytrap/honeytrap.log

Step 3: Testing & Attack Simulation

1. Port Scanning (Simulate Attacker)

Run an **Nmap** scan to detect open ports:

nmap -sV -p 2222 <your-ip>

2. Simulating Brute-Force Attack

Use **Hydra** to simulate brute-force login attempts:

hydra -l admin -P rockyou.txt ssh://<your-ip> -s 2222

3. Monitor Logs in Real-time

tail -f /var/log/honeytrap/honeytrap.log

Step 4: Log Analysis & Reporting

1. **Extract Unique IPs from Attackers**

cat /var/log/honeytrap/honeytrap.log | grep "Connection from" | awk '{print $4}' | sort | uniq -c

2. **Use ELK Stack for Advanced Log Analysis**
    - Install **Elasticsearch, Logstash, Kibana**
    - Set up a pipeline to parse logs
    - Visualize attack patterns

Test Setup

Environment Details

- **Operating System:** Kali Linux
- **Honeypot Tool:** HoneyTrap
- **Logging Mechanism:** Default HoneyTrap logs + ELK Stack for visualization
- **Testing Tools:** Nmap, Hydra (for brute-force attack simulation)
- **Network Configuration:** Localhost setup with exposed SSH service on port 2222

The HoneyTrap configuration (`/etc/honeytrap/honeytrap.conf`) is set as follows:

```
[listener]
type = "tcp"
listen = ":2222"

[services.ssh]
enabled = true
logdir = "/var/log/honeytrap"
```

HoneyTrap was started using:

sudo honeytrap -c /etc/honeytrap/honeytrap.conf

Port Scanning Test (Nmap)

Objective: Identify open ports and services exposed by HoneyTrap.

nmap -sV -p 2222 <target-ip>

Expected Result: The honeypot should respond as an active SSH service. **Actual Result:** Nmap detected the port as open with SSH service.

Brute-Force Attack Simulation (Hydra)

Objective: Simulate an attacker attempting to brute-force SSH credentials.

hydra -l admin -P rockyou.txt ssh://<target-ip> -s 2222

Expected Result: The honeypot should log multiple authentication attempts. **Actual Result:** Logs captured the attacker's repeated login attempts.

Log Monitoring

To observe live attack logs:

tail -f /var/log/honeytrap/honeytrap.log

Sample log entry:

[INFO] Connection from 192.168.1.10 to port 2222

[ALERT] Multiple failed login attempts detected from 192.168.1.10

Results & Findings

- **Detected Attack Sources:**

cat /var/log/honeytrap/honeytrap.log | grep "Connection from" | awk '{print $4}' | sort | uniq -c

- **Attack Trends:** Analyzed using the ELK Stack to visualize attack frequency and sources.
