

honeypot_implementation_sop

Honeypot Inplementazioa eta Konfigurazioa - SOP

Helburua

Honeypot bat ezartzeko eta kudeatzeko prozedura, erasoen detekzioa eta analisisa egiteko, batez ere OT/Industrial sektorerara bideratua.

Aurrebaldintzak

- Docker eta Docker Compose instalatuta
- SIEM sistema (ELK Stack) ezarrita
- Sareko firewall-a ezarrita
- VM edo hardware espezifikoa honeypot-erako

1. Honeypot Mota Aukeraketa

1.1 Interakzio Baxuko Honeypot-ak

- **Honeyd:** TCP/IP protokoloak simulatzen ditu
- **Dionaea:** Malware eta exploit-ak harrapatzen ditu
- **Cowrie:** SSH eta FTP honeypot

1.2 Interakzio Ertain/Altuko Honeypot-ak

- **Conpot:** ICS/SCADA honeypot (Siemens S7, Modbus, etab.)
- **Kippo:** SSH honeypot
- **Glastopf:** Web application honeypot

1.3 Honeypot Industrialak

- **Conpot:** ICS protokoloak simulatzen ditu
- **SCADA-Honeynet:** SCADA sistemak simulatzen ditu

2. Conpot Honeypot Ezartzea (Industrial)

2.1 Docker bidez instalatu

docker pull honeytrap/honeytrap

docker run -d --name conpot -p 102:102 -p 502:502 -p 8080:8080 conpot/conpot

2.2 Konfigurazioa

nano /opt/conpot/templates/default/template.xml

2.3 Template-a Pertsonalizatu

```

<template>
  <host>
    <name>Zabala Gailetak PLC</name>
    <mac>00:0C:29:12:34:56</mac>
    <ip>192.168.50.10</ip>
  </host>

  <services>
    <modbus port="502">
      <port>502</port>
      <unit_id>1</unit_id>
      <registers>
        <register address="40001" value="100"/>
        <register address="40002" value="200"/>
      </registers>
    </modbus>

    <s7comm port="102">
      <port>102</port>
      <module_type>CPU 315-2 DP</module_type>
    </s7comm>

    <http port="8080">
      <port>8080</port>
      <path>/</path>
      <status>200</status>
      <content>text/html</content>
      <body>
        <html>
          <body>
            <h1>Zabala Gailetak - PLC Interface</h1>
            <p>Unauthorized access prohibited</p>
          </body>
        </html>
      </body>
    </http>
  </services>
</template>

```

3. Cowrie SSH Honeypot Ezartzea

3.1 Docker Compose erabili

```

version: '3'
services:
  cowrie:
    image: cowrie/cowrie
    container_name: cowrie
    ports:
      - "2222:2222"
      - "2223:2223"
    volumes:
      - ./cowrie/cowrie.cfg:/home/cowrie/cowrie-git/cowrie/cowrie.cfg
      - ./cowrie/fs.pickle:/home/cowrie/cowrie-git/cowrie/fs.pickle
      - ./cowrie/etc:/home/cowrie/cowrie-git/cowrie/etc
      - ./cowrie/log:/home/cowrie/cowrie-git/cowrie/log
    networks:
      - honeypot-net

networks:
  honeypot-net:
    driver: bridge

```

3.2 Konfigurazioa

```
[cowrie]
hostname = zabalagailetak-pc-01
ssh_version = SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3
listen_endpoints = tcp:2222:interface=0.0.0.0
```

```
[output_json]
logfile = log/cowrie.json
```

```
[output_mysql]
enabled = true
host = 192.168.200.10
database = honeypot
username = cowrie
password = secure_password
```

4. Dionaea Malware Honeydota

4.1 Instalazioa

```
docker run -d --name dionaea -p 21:21 -p 42:42 -p 135:135 -p 445:445 -p
1433:1433 -p 3306:3306 -p 80:80 -p 443:443 -v ./dionaea:/var/dionaea
honeypot/dionaea
```

4.2 Konfigurazioa

dionaea:

listen:

tcp:

- address: "0.0.0.0"
- port: 21
- address: "0.0.0.0"
- port: 445
- address: "0.0.0.0"
- port: 3306
- address: "0.0.0.0"
- port: 80
- address: "0.0.0.0"
- port: 443

downloads:

dir: /var/dionaea/downloads

log:

file: /var/dionaea/log/dionaea.log
level: info

submit:

- http://virustotal.com/api/submit

5. Sarearen Konfigurazioa

5.1 DMZ-a Honeydota-erako

```
iptables -A INPUT -p tcp --dport 102 -j DNAT --to-destination 192.168.100.50:102
iptables -A INPUT -p tcp --dport 502 -j DNAT --to-destination 192.168.100.50:502
iptables -A INPUT -p tcp --dport 2222 -j DNAT --to-destination
192.168.100.51:2222
```

5.2 NAT eta Port Forwarding

```
iptables -t nat -A PREROUTING -d EXTERNAL_IP -p tcp --dport 22 -j DNAT --to
192.168.100.51:2222
```

6. Logging eta SIEM Integrazioa

6.1 Logstash Konfigurazioa

```
input {
  file {
    path => "/var/log/honeypot/*.log"
    type => "honeypot"
    start_position => "beginning"
  }
}

filter {
  if [type] == "honeypot" {
    grok {
      match => {
        "message" => "%{TIMESTAMP_ISO8601:timestamp} %{LOGLEVEL:level}
%{GREEDYDATA:msg}"
      }
    }

    geoip {
      source => "[src_ip]"
    }
  }
}

output {
  elasticsearch {
    hosts => ["http://elasticsearch:9200"]
    index => "honeypot-%{+YYYY.MM.dd}"
  }
}
```

6.2 Kibana Dashboard-a Sortu

- IP helbideen mapa
- Eraso moten diagramak
- Geolokalizazioa
- Time-series grafikoak
- Top erasotzaileak

7. Alertak

7.1 Threshold Alert-ak

```
import elasticsearch

es = elasticsearch.Elasticsearch(['http://elasticsearch:9200'])

def check_threshold():
    query = {
        "query": {
            "range": {
                "@timestamp": {
                    "gte": "now-1h"
                }
            }
        }
    }

    result = es.search(index="honeypot-*", body=query)
```

```
if result['hits']['total']['value'] > 100:
    send_alert("Eraso kopuru handia detektatu da honeypot-en")
```

7.2 Slack Jakinarazpena

```
import requests
```

```
def send_slack_alert(message):
    webhook_url = "SLACK_WEBHOOK_URL"
    payload = {"text": message}
    requests.post(webhook_url, json=payload)
```

8. Analisia eta Txostena

8.1 Eguneko Txostena

```
def generate_daily_report():
    report = {
        "date": datetime.now().strftime("%Y-%m-%d"),
        "total_attacks": count_total_attacks(),
        "attack_types": count_by_type(),
        "top_sources": get_top_sources(),
        "malware": get_malware_samples()
    }

    save_report(report)
```

8.2 Asteko Analisia

- Eraginaren analisia
- Joerak identifikatu
- Zero-day detekzioak
- Inteligentzia kanpotik partekatu

9. Kudeaketa eta Mantentzea

9.1 Log-en Rotazioa

```
/var/log/honeypot/*.log {
    daily
    rotate 30
    compress
    delaycompress
    missingok
    notifempty
    create 0640 honeypot honeypot
}
```

9.2 Backup-ak Sortu

```
tar -czf honeypot-backup-$(date +%Y%m%d).tar.gz /opt/honeypot/
```

10. Segurtasun Neurriak

10.1 Honeypot-aren Isolazioa

- Sare isolatu batean jarri
- Firewall rules zorrotzak

- Ez erabili ekoizpeneko sarean
- Ez partekatu kredentzialak

10.2 Legera Etika

- Honeypot-aren erabilpena dokumentatu
- Erabilera politikak definitu
- Pribatutasun legeak kontuan hartu
- Consent eta notifikazioak

11. Errendimenduaren Monitorizazioa

11.1 Baliabideen Erabilera

docker stats conpot cowrie dionaea

11.2 Auto-eskala

12. Difusioa eta Inteligentzia

12.1 Mehatxu Inteligentzia Partekatu

- MISP erabili
- TAXII erabili
- CERT-ak informatu
- Community partekatu

12.2 Ikaskuntzak Aplikatu

- Honeypot-en ikasitakoak ekoizpenean aplikatu
- Firewall rules eguneratu
- Signature-ak gehitu
- IPS rules eguneratu

Erreferentziak

- Honeynet Project: <https://www.honeynet.org/>
- Conpot Documentation: <https://conpot.readthedocs.io/>
- Cowrie Documentation: <https://cowrie.readthedocs.io/>
- Dionaea Documentation: <https://dionaea.readthedocs.io/>
- MISP Project: <https://www.misp-project.org/>