

# Informe de Pruebas Técnicas – SotyPot



## 1. Introducción

Este documento describe la batería completa de pruebas de validación realizadas sobre la plataforma de honeypots SotyPot. Las pruebas se ejecutaron desde una máquina Kali Linux con el fin de comprobar la capacidad de detección, registro y análisis de eventos maliciosos reales en un entorno controlado.

```
soty-attacker@Soty-attacker: ~  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g  
roup default qlen 1000  
    link/ether c6:fb:c6:71:1c:b9 brd ff:ff:ff:ff:ff:ff  
    inet 172.26.0.66/16 brd 172.26.255.255 scope global dynamic noprefixroute  
        eth0  
        valid_lft 551sec preferred_lft 551sec  
    inet6 fe80::c6fb:c6ff:fe71:1cb9/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
soty-attacker@Soty-attacker: ~  
$ ping 172.26.0.11  
PING 172.26.0.11 (172.26.0.11) 56(84) bytes of data.  
64 bytes from 172.26.0.11: icmp_seq=1 ttl=64 time=1.30 ms  
64 bytes from 172.26.0.11: icmp_seq=2 ttl=64 time=0.361 ms  
64 bytes from 172.26.0.11: icmp_seq=3 ttl=64 time=0.419 ms  
--- 172.26.0.11 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2031ms  
rtt min/avg/max/mdev = 0.361/0.693/1.300/0.429 ms  
soty-attacker@Soty-attacker: ~  
$
```

## 2. Herramientas Empleadas

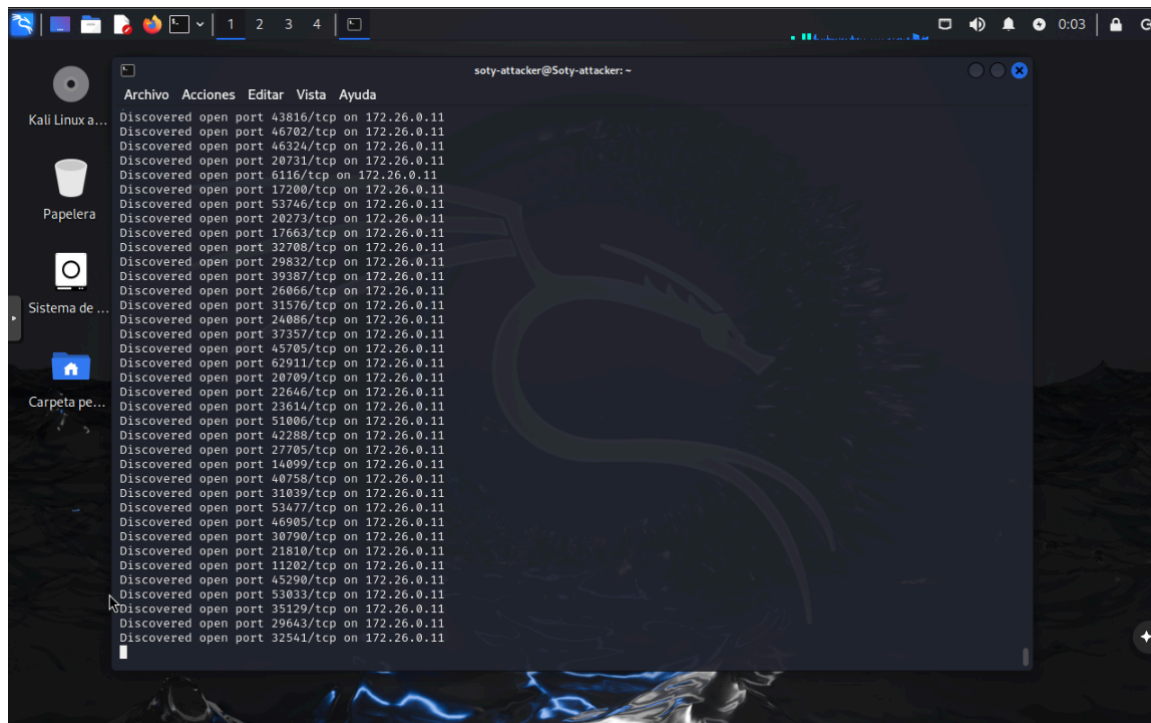
Herramienta	Función
nmap	Escaneo de red, fingerprinting de puertos
hydra	Ataques de fuerza bruta sobre SSH
curl	Peticiones web HTTP
whois	Consulta de información IP
nikto	Escaneo de vulnerabilidades web
msfconsole	Simulación de explotación controlada

## 3. Pruebas Realizadas

### 3.1 Escaneo Nmap Avanzado

*Comando utilizado:*

```
nmap -A -T4 -p- -v <IP_SOTYPOT>
```

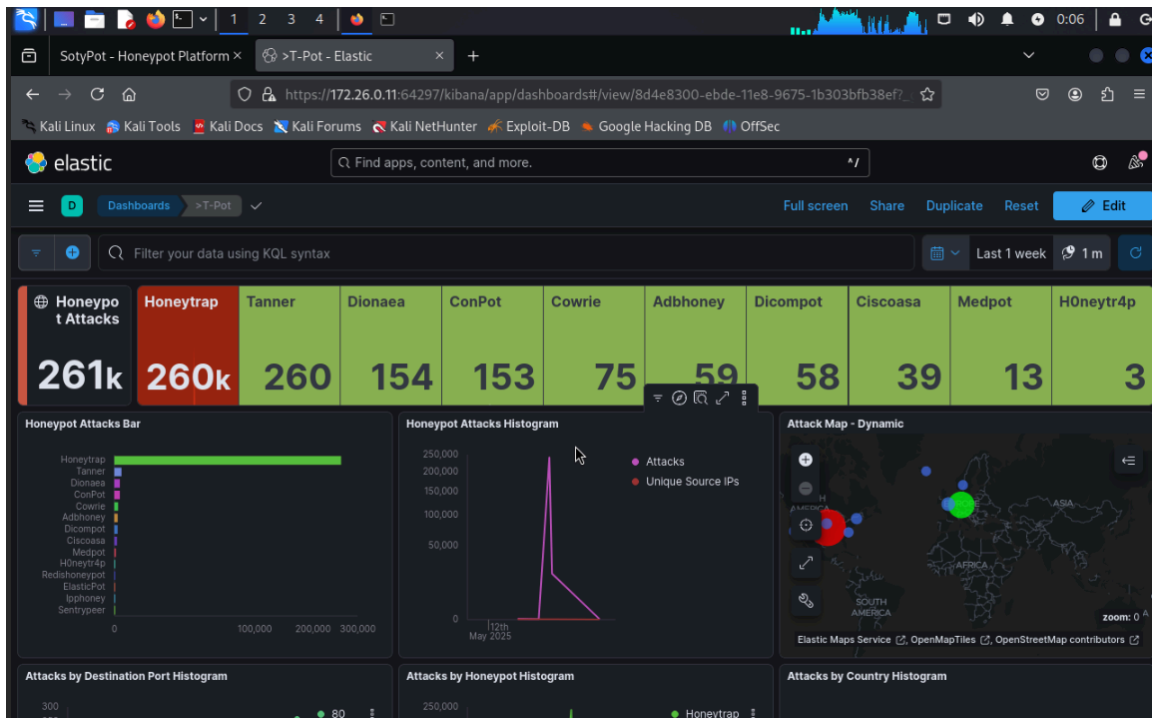


```
(soty-attacker@Soty-attacker)-[~]
$ nmap -A -T4 -p- -v 172.26.0.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-18 00:03 CEST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:03
Completed NSE at 00:03, 0.00s elapsed
Initiating NSE at 00:03
Completed NSE at 00:03, 0.00s elapsed
Initiating NSE at 00:03
Completed NSE at 00:03, 0.00s elapsed
Initiating ARP Ping Scan at 00:03
Scanning 172.26.0.11 [1 port]
Completed ARP Ping Scan at 00:03, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:03
Completed Parallel DNS resolution of 1 host. at 00:03, 0.01s elapsed
Initiating SYN Stealth Scan at 00:03
Scanning 172.26.0.11 [65535 ports]
Discovered open port 443/tcp on 172.26.0.11
Discovered open port 445/tcp on 172.26.0.11
Discovered open port 135/tcp on 172.26.0.11
Discovered open port 21/tcp on 172.26.0.11
Discovered open port 25/tcp on 172.26.0.11
Discovered open port 22/tcp on 172.26.0.11
Discovered open port 5900/tcp on 172.26.0.11
Discovered open port 8080/tcp on 172.26.0.11
Discovered open port 80/tcp on 172.26.0.11
```

```
soty-attacker@Soty-attacker: ~
Archivo Acciones Editar Vista Ayuda
Discovered open port 39830/tcp on 172.26.0.11
Discovered open port 8779/tcp on 172.26.0.11
Discovered open port 1183/tcp on 172.26.0.11
Discovered open port 17368/tcp on 172.26.0.11
Discovered open port 11038/tcp on 172.26.0.11
Discovered open port 9302/tcp on 172.26.0.11
Discovered open port 50784/tcp on 172.26.0.11
Discovered open port 39440/tcp on 172.26.0.11
Discovered open port 61103/tcp on 172.26.0.11
Discovered open port 57826/tcp on 172.26.0.11
Discovered open port 39259/tcp on 172.26.0.11
Discovered open port 52576/tcp on 172.26.0.11
Discovered open port 6836/tcp on 172.26.0.11
Discovered open port 36265/tcp on 172.26.0.11
Discovered open port 45886/tcp on 172.26.0.11
Discovered open port 23292/tcp on 172.26.0.11
Discovered open port 6608/tcp on 172.26.0.11
Discovered open port 51240/tcp on 172.26.0.11
Discovered open port 35089/tcp on 172.26.0.11
Discovered open port 55319/tcp on 172.26.0.11
Discovered open port 7998/tcp on 172.26.0.11
Discovered open port 57771/tcp on 172.26.0.11
Discovered open port 63918/tcp on 172.26.0.11
Discovered open port 40583/tcp on 172.26.0.11
Discovered open port 36341/tcp on 172.26.0.11
Discovered open port 53014/tcp on 172.26.0.11
Discovered open port 4534/tcp on 172.26.0.11
SYN Stealth Scan Timing: About 15.99% done; ETC: 00:12 (0:07:27 remaining)
SYN Stealth Scan Timing: About 16.44% done; ETC: 00:15 (0:09:45 remaining)
SYN Stealth Scan Timing: About 17.33% done; ETC: 00:17 (0:11:32 remaining)
Discovered open port 6379/tcp on 172.26.0.11
Discovered open port 465/tcp on 172.26.0.11
SYN Stealth Scan Timing: About 18.20% done; ETC: 00:19 (0:13:07 remaining)
SYN Stealth Scan Timing: About 19.09% done; ETC: 00:21 (0:14:29 remaining)

(soty-attacker@Soty-attacker)-[~]
$
```

### Resultado esperado:

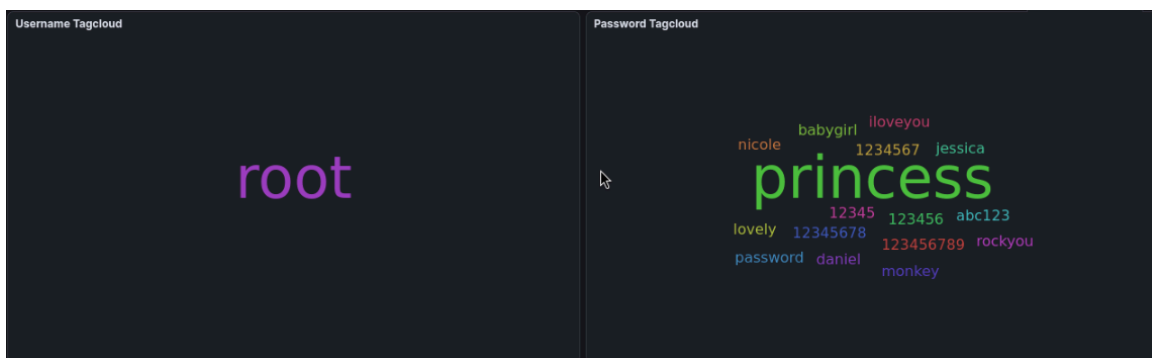
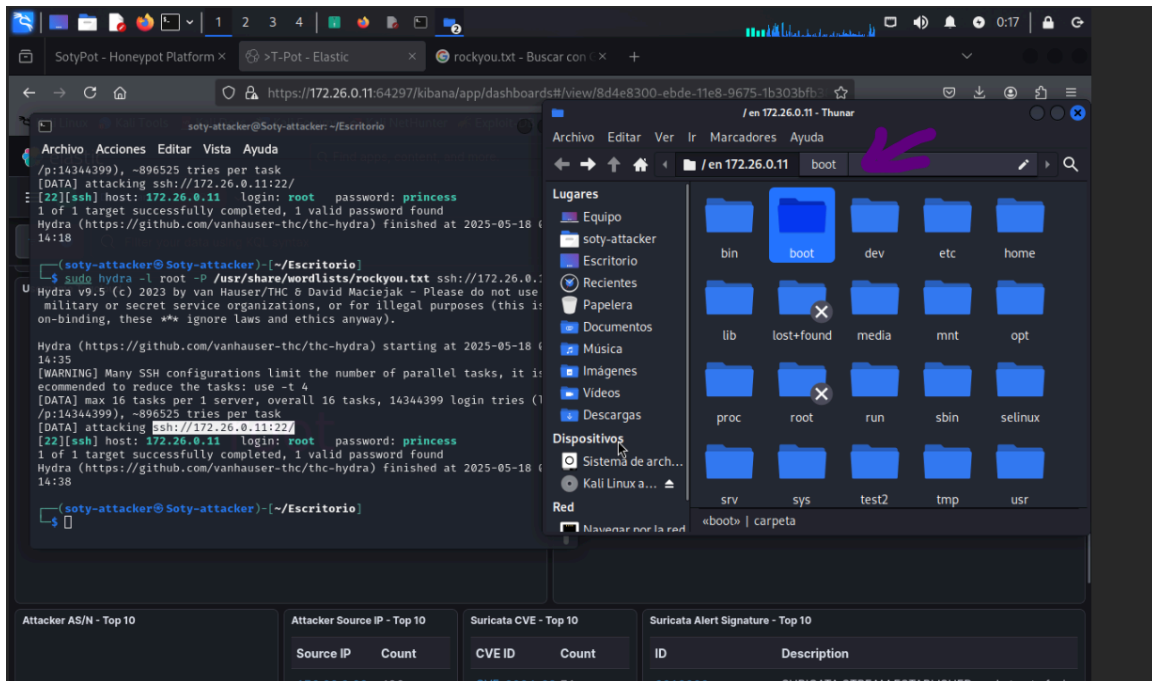


Honeypots como Dionaea y Suricata detectaron el escaneo masivo. Los eventos se reflejaron en los dashboards de Kibana con logs enriquecidos.

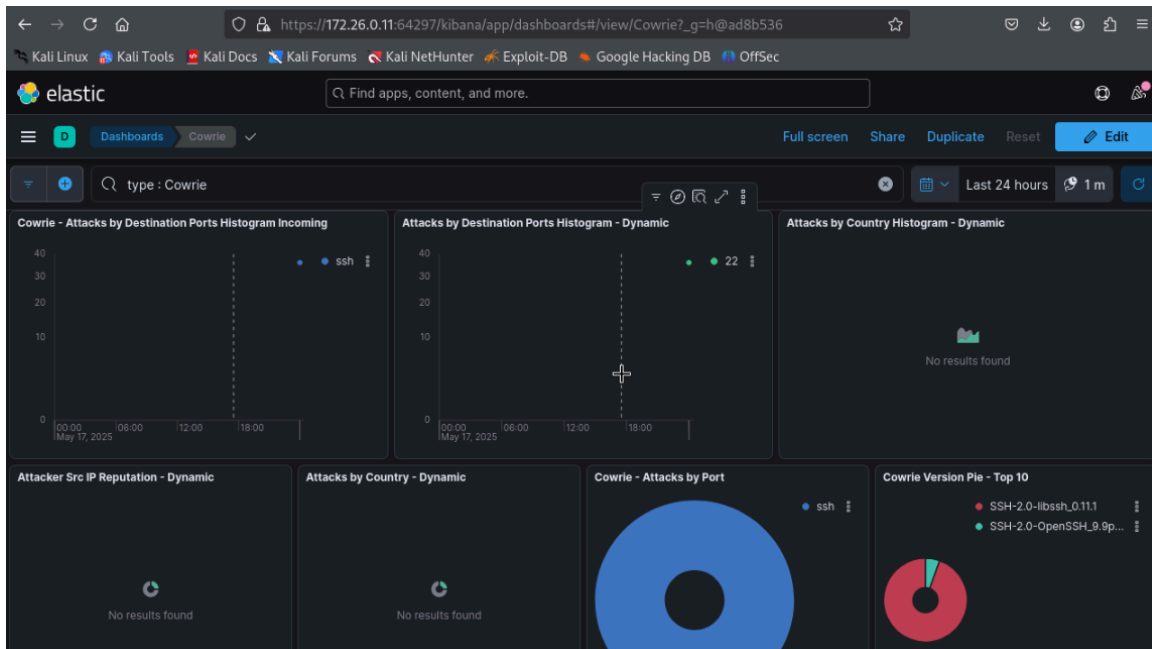
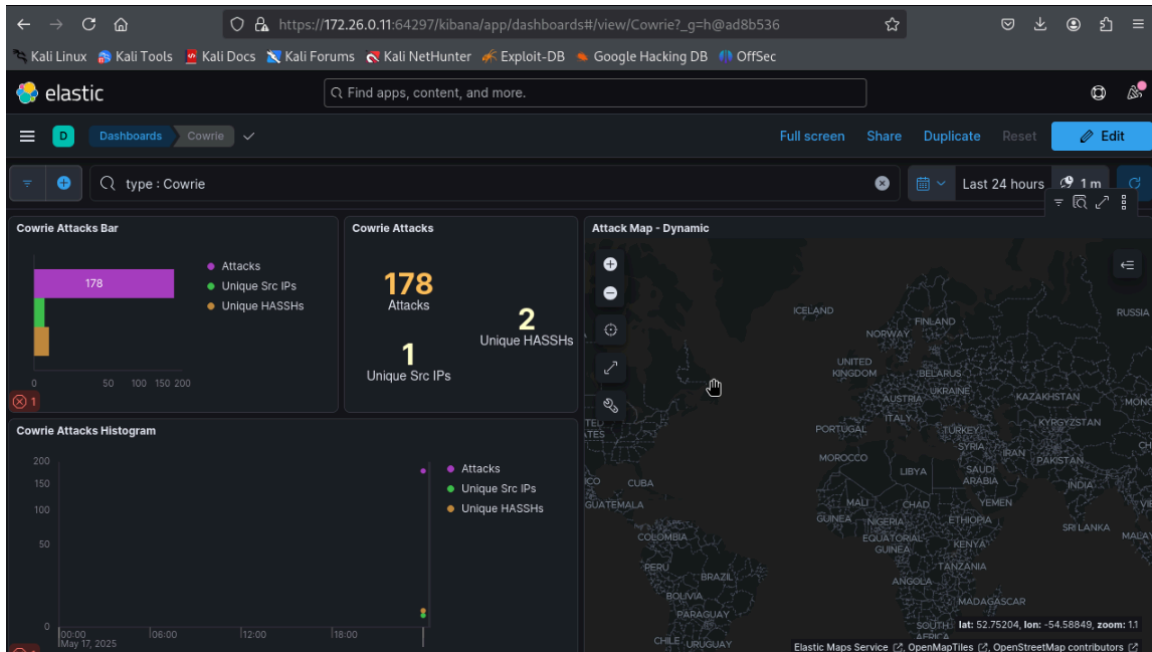
## 3.2 Fuerza Bruta SSH con Hydra

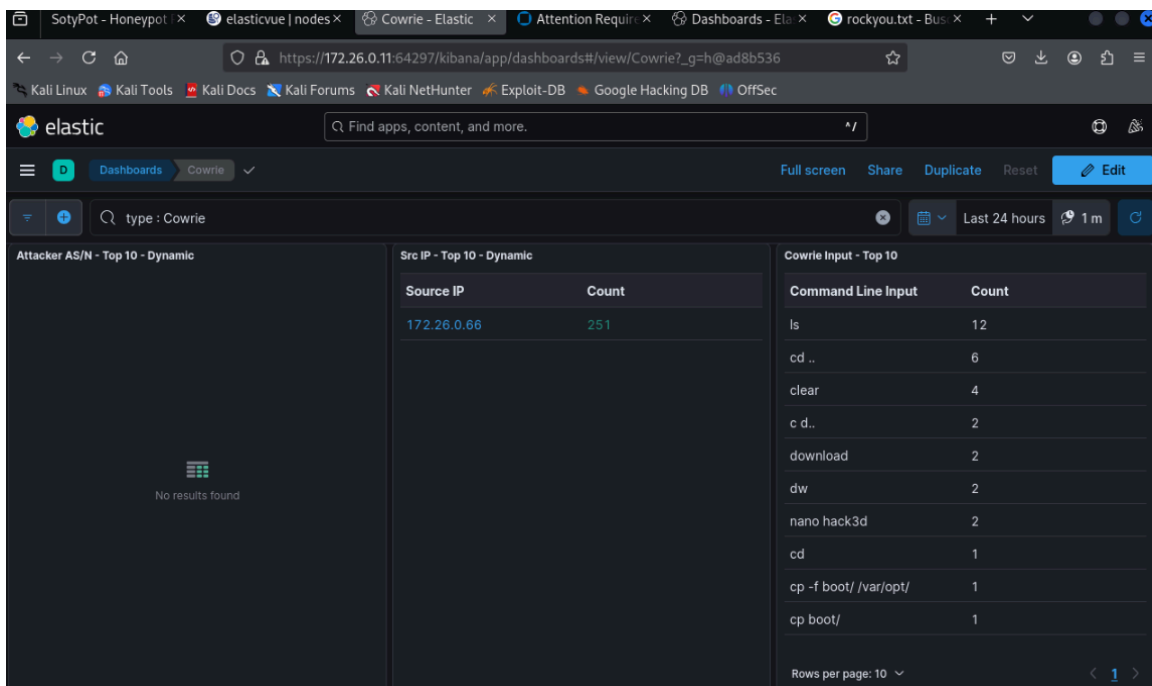
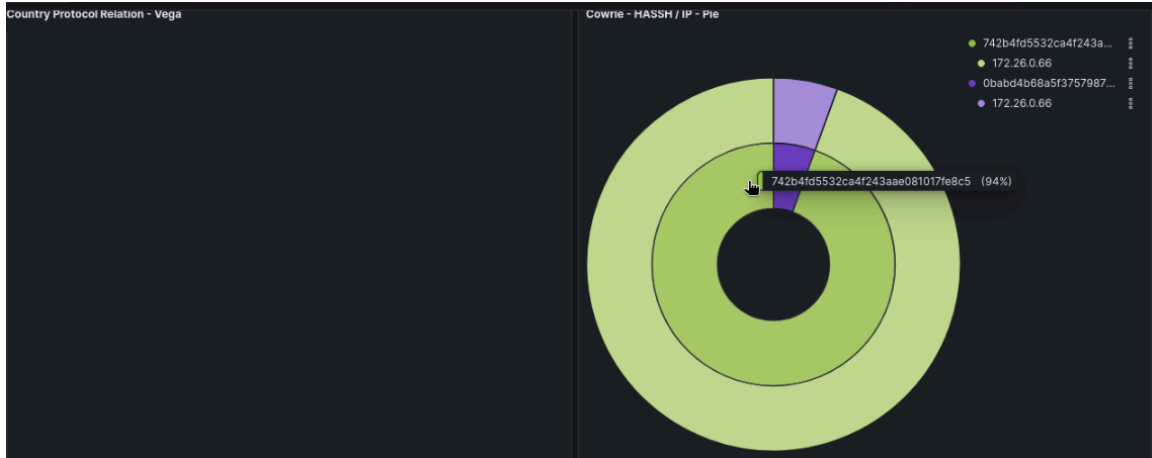
### Comando utilizado:

hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://<IP\_SOTYPOT>



### Resultado esperado:





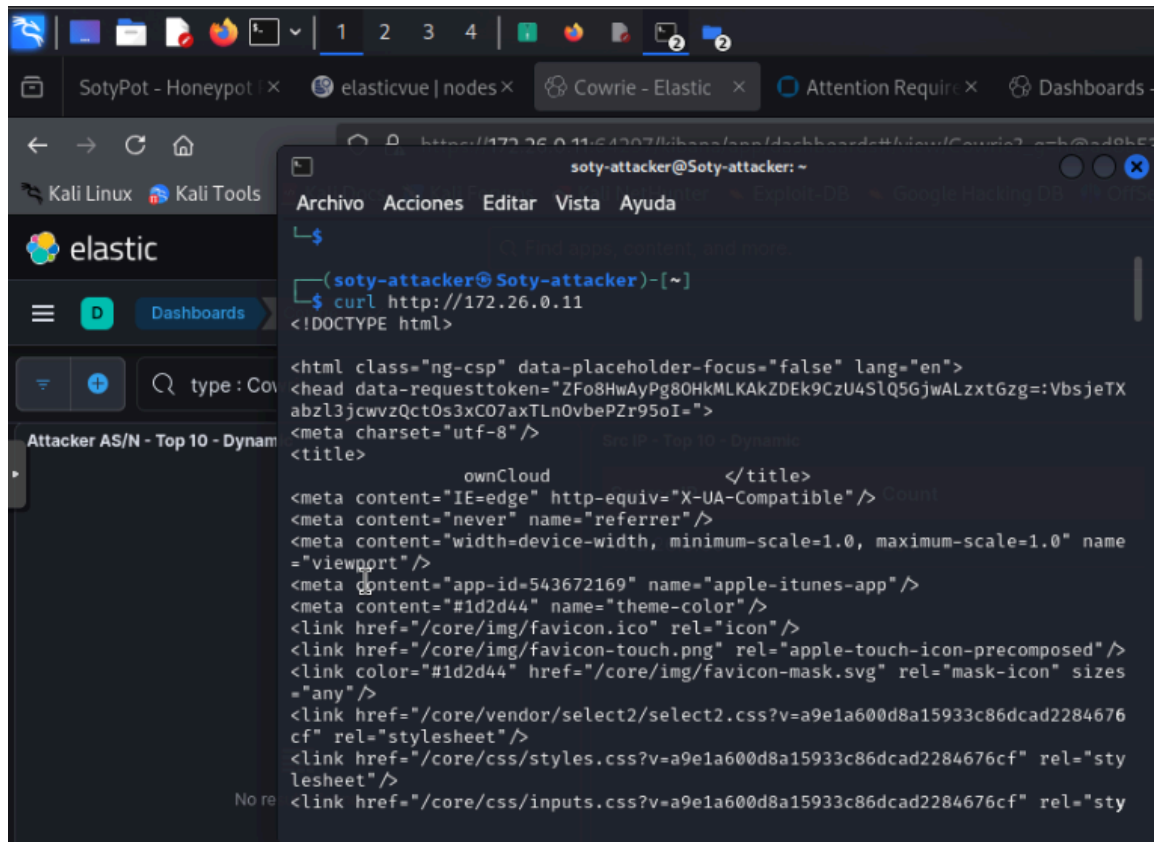
Cowrie registró cada intento de login incluyendo credenciales, IP, timestamp y comandos simulados.



### 3.3 Acceso HTTP con curl

#### *Comando utilizado:*

curl http://<IP\_SOTYPOT>

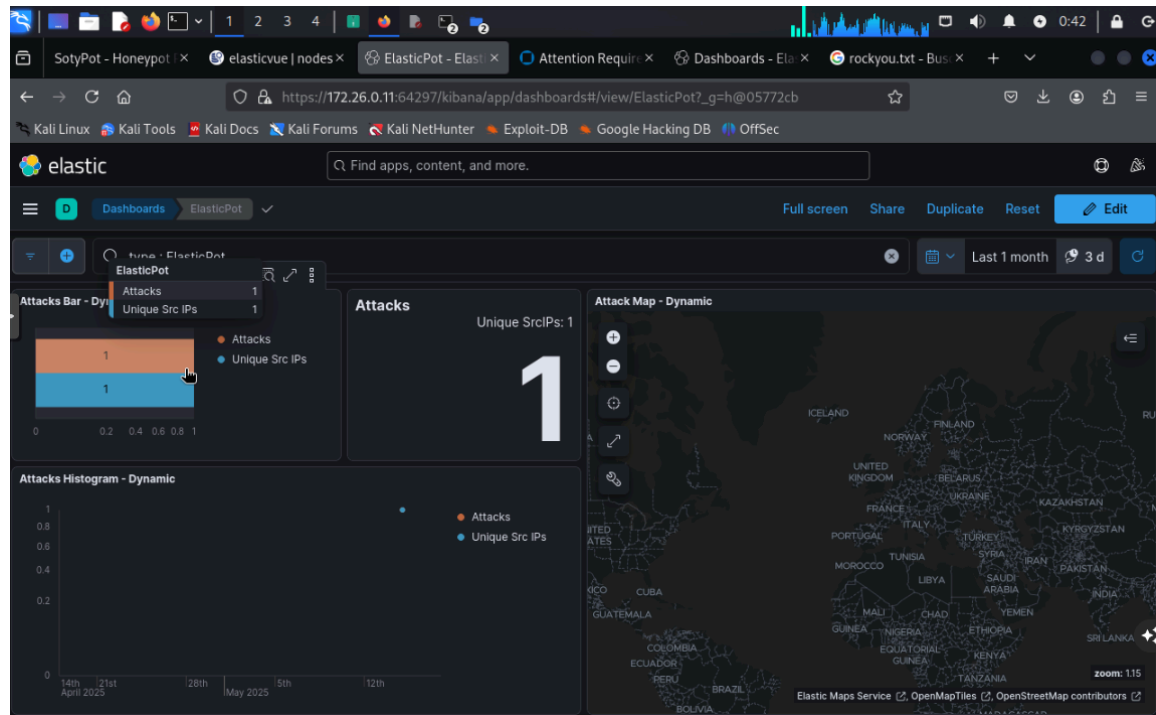


```
soty-attacker@Soty-attacker: ~  
$ curl http://172.26.0.11  
<!DOCTYPE html>  
  
<html class="ng-csp" data-placeholder-focus="false" lang="en">  
<head data-requesttoken="ZFo8HwAyPg80HkMLKAKZDEk9CzU4SlQ5GjwALzxtGzg=:VbsjeTX  
abzl3jcwvzQctOs3xC07axTLn0vbePZr95oI=">  
<meta charset="utf-8" />  
<title>  
    ownCloud  
</title>  
<meta content="IE=edge" http-equiv="X-UA-Compatible" />  
<meta content="never" name="referrer" />  
<meta content="width=device-width, minimum-scale=1.0, maximum-scale=1.0" name  
="viewport" />  
<meta content="app-id=543672169" name="apple-itunes-app" />  
<meta content="#1d2d44" name="theme-color" />  
<link href="/core/img/favicon.ico" rel="icon" />  
<link href="/core/img/favicon-touch.png" rel="apple-touch-icon-precomposed" />  
<link color="#1d2d44" href="/core/img/favicon-mask.svg" rel="mask-icon" sizes  
="any" />  
<link href="/core/vendor/select2/select2.css?v=a9e1a600d8a15933c86dcad2284676  
cf" rel="stylesheet" />  
<link href="/core/css/styles.css?v=a9e1a600d8a15933c86dcad2284676cf" rel="sty  
lesheet" />  
<link href="/core/css/inputs.css?v=a9e1a600d8a15933c86dcad2284676cf" rel="sty
```

#### *Resultado esperado:*

Wordpot y Elasticpot capturaron peticiones HTTP básicas, reflejadas como eventos en Elasticsearch.





### 3.4 Escaneo Web con Nikto

*Comando utilizado:*

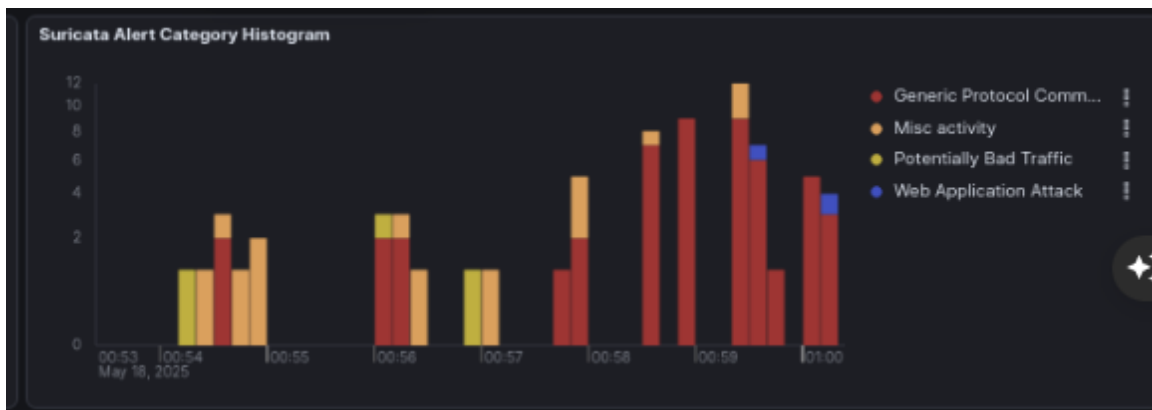
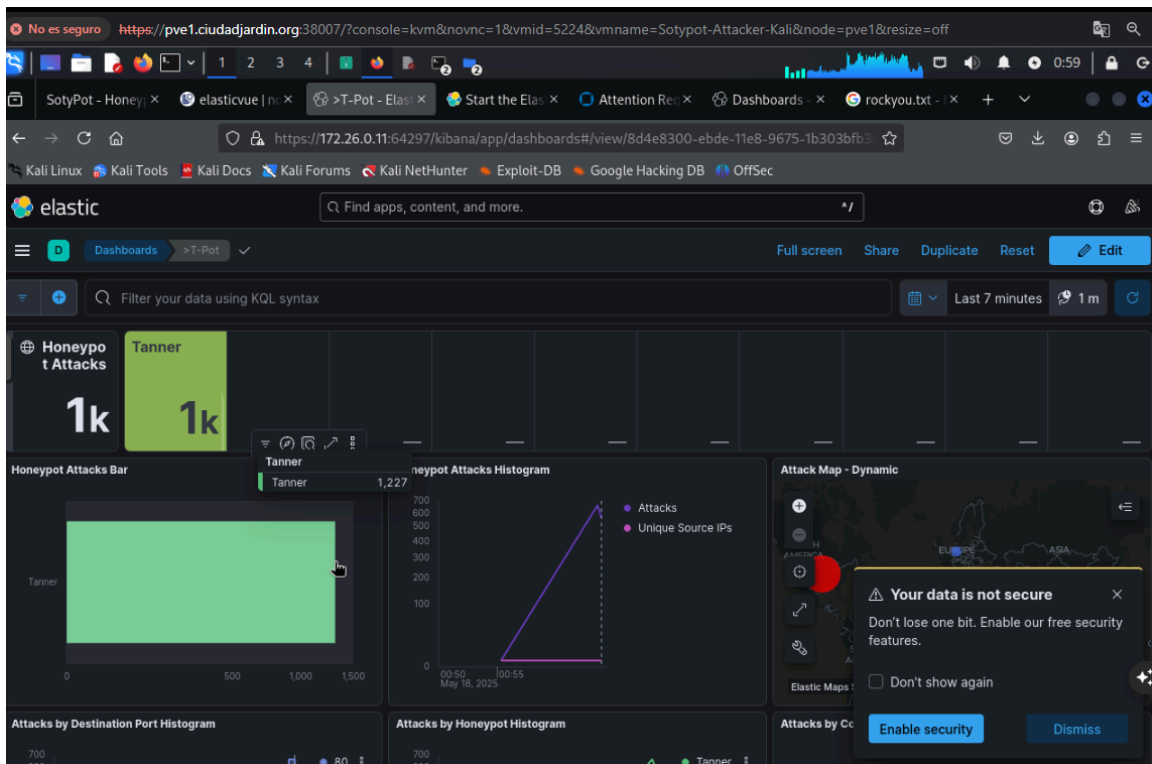
nikto -h http://<IP\_SOTYPOT>

```
(soty-attacker@Soty-attacker)-[~/Escritorio]
$ nikto -h http://172.26.0.11
- Nikto v2.5.0

+ Target IP: 172.26.0.11
+ Target Hostname: 172.26.0.11
+ Target Port: 80
+ Start Time: 2025-05-18 00:47:01 (GMT2)

+ Server: Python/3.11 aiohttp/3.8.6
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
```

### Resultado esperado:

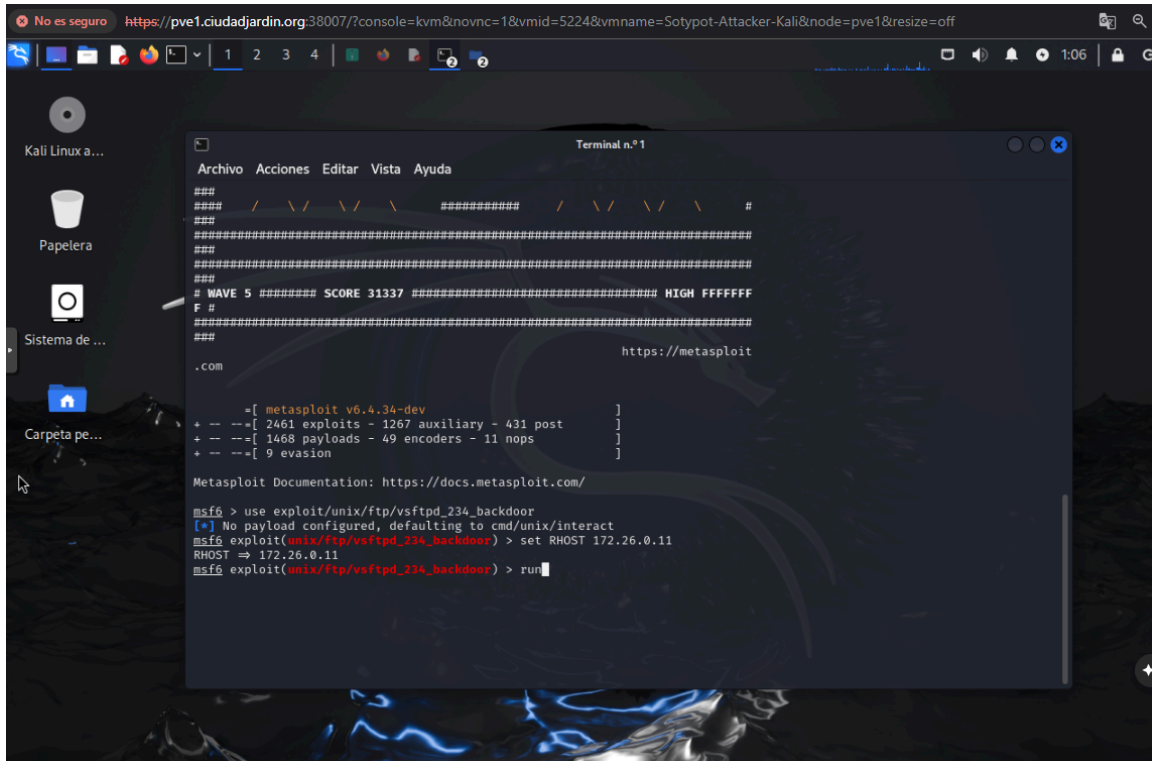


Las rutas escaneadas fueron detectadas y almacenadas en logs accesibles por Kibana.

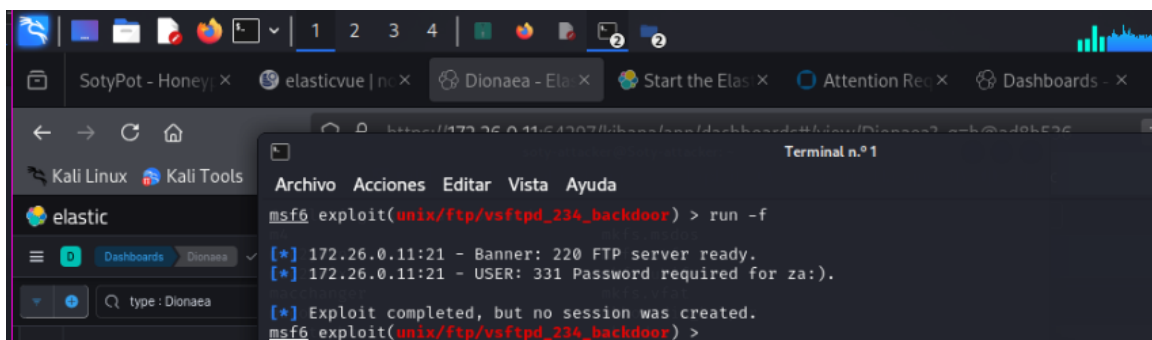
### 3.5 Simulación de Exploit con Metasploit

#### Comando utilizado:

use exploit/unix/ftp/vsftpd\_234\_backdoor  
set RHOST <IP\_SOTYPOT>  
run

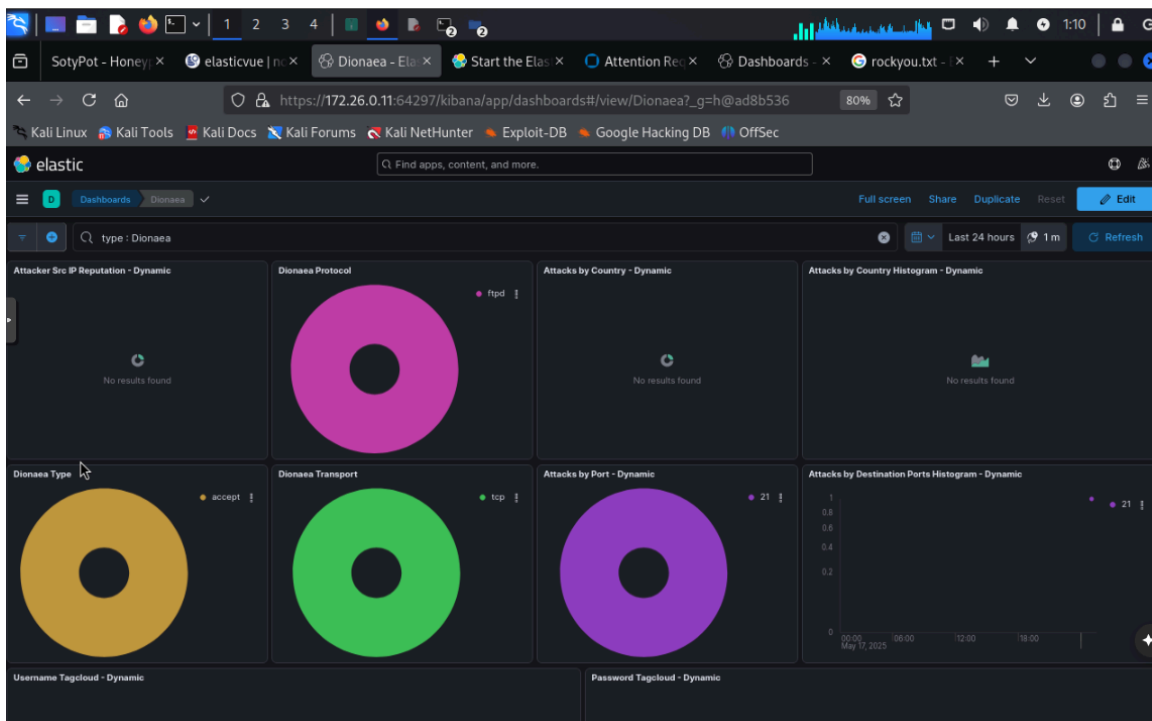
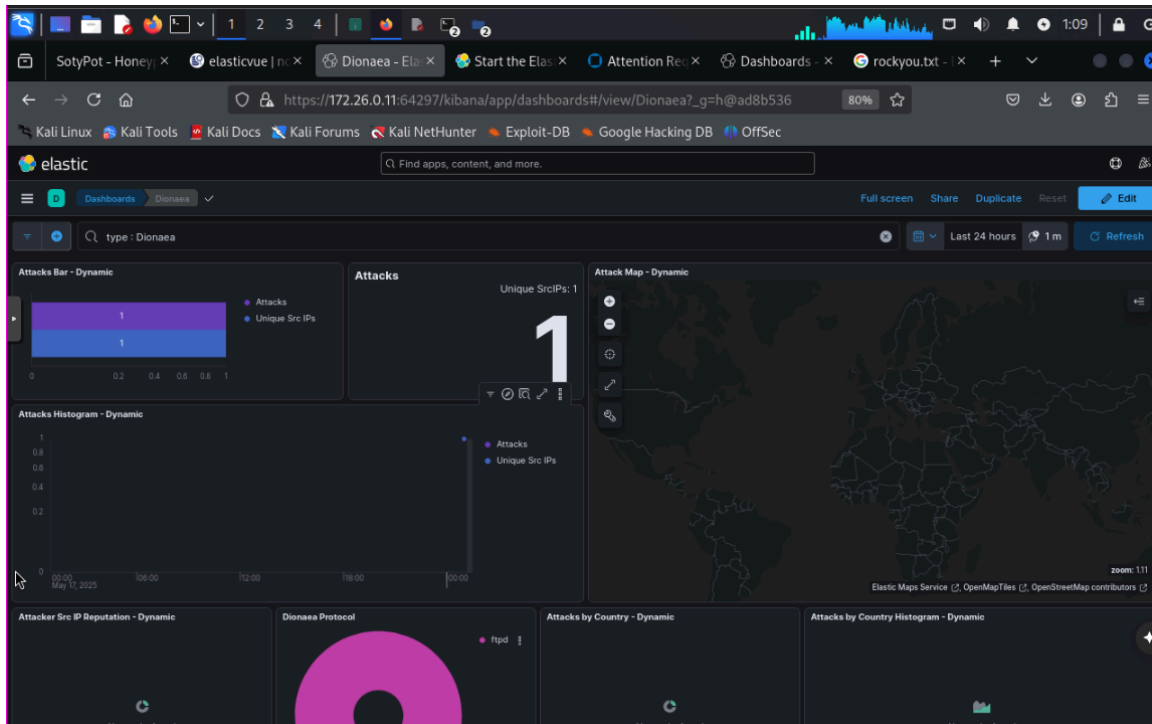


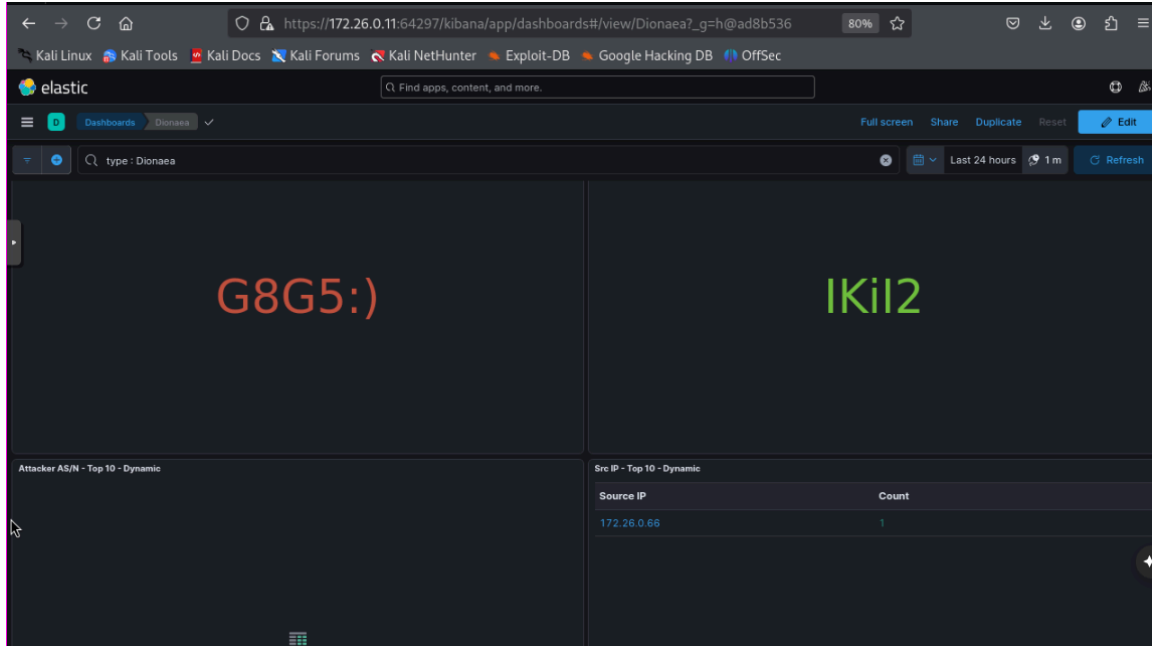
The screenshot shows a Kali Linux desktop with a terminal window titled 'Terminal n.º 1'. The terminal displays the Metasploit Meterpreter (msf6) interface. It shows the command 'use exploit/unix/ftp/vsftpd\_234\_backdoor' being executed, followed by 'set RHOST 172.26.0.11' and 'run'. The output shows the exploit details, including the number of exploits, auxiliary, post, payloads, encoders, and nops. It also shows the Metasploit Documentation URL: <https://docs.metasploit.com/>.



The screenshot shows a Kali Linux desktop with a terminal window titled 'Terminal n.º 1' and a web browser window. The terminal displays the command 'run -f' being executed, followed by the output: '[\*] 172.26.0.11:21 - Banner: 220 FTP server ready. [\*] 172.26.0.11:21 - USER: 331 Password required for za:). [\*] Exploit completed, but no session was created.' The web browser window shows the URL 'http://172.26.0.11:21/220-FTP-server-ready/331-Password-required-for-za:)' and the page content 'Dionaea - Ela...'. The browser also shows the 'elastic' dashboard and the 'Dionaea' tool.

### Resultado esperado:





El intento de explotación fue detectado por Dionaea y registrado como intento de conexión sospechosa.

#### 4. Análisis de Resultados

SotyPot respondió adecuadamente a todos los intentos de acceso, escaneo y explotación. Las herramientas de visualización como Kibana mostraron en tiempo real los eventos con información enriquecida que permite el análisis forense y educativo. La segmentación por servicio (SSH, HTTP, FTP, etc.) ayuda a clasificar el tipo de amenaza simulada.

#### 5. Resumen de Detección

Prueba	Detectado	Registrado	Visualizado	Alertado
Nmap -A	✓	✓	✓	⚠️
Hydra SSH	✓	✓	✓	✓
curl HTTP	✓	✓	✓	✗
Nikto	✓	✓	✓	⚠️
Metasploit FTP	✓	✓	✓	⚠️

## 6. Conclusión Técnica

El entorno SotyPot permite realizar pruebas ofensivas simuladas de forma segura, recogiendo evidencia en tiempo real que demuestra su efectividad como herramienta de detección y formación. Todas las pruebas documentadas pueden ser repetidas por cualquier usuario con acceso a una red de pruebas, y las evidencias visuales pueden ser añadidas fácilmente mediante capturas de pantalla de los dashboards.

## 7. Bibliografía

1. Telekom Security. (2024). *T-Pot CE - The All In One Multi Honeypot Platform*. Recuperado de: <https://github.com/telekom-security/tpotce>
2. Elastic.co. (2024). *Elastic Stack Documentation (Elasticsearch, Logstash, Kibana)*. Recuperado de: <https://www.elastic.co/guide>
3. Grafana Labs. (2024). *Grafana Documentation*. Recuperado de: <https://grafana.com/docs>
4. Docker Inc. (2024). *Docker & Docker Compose Official Documentation*. Recuperado de: <https://docs.docker.com>
5. Nmap Project. (2024). *Nmap Reference Guide*. Recuperado de: <https://nmap.org/book/man-briefoptions.html>
6. OWASP Foundation. (2024). *OWASP Honeypots Project*. Recuperado de: <https://owasp.org/www-community/Honeypots>
7. Offensive Security. (2024). *Kali Linux Tools Documentation*. Recuperado de: <https://tools.kali.org>
8. GitHub - descambiado. (2025). *SotyPot - Honeypot educativo basado en T-Pot CE*. Recuperado de: <https://github.com/descambiado/SotyPot>
9. Vacca, J. R. (2022). *Computer and Information Security Handbook* (4th ed.). Academic Press.
10. Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94. U.S. Department of Commerce.

Este trabajo se distribuye bajo la licencia Creative Commons

Attribution-NonCommercial-ShareAlike 4.0 International.

(<http://creativecommons.org/licenses/by-nc-sa/4.0/>)