# UNIVERSIDAD DE LAS FUERZAS ARMADAS - "ESPE"

**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES**
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

## "ANÁLISIS DE LAS VULNERABILIDADES DE SEGURIDAD INFORMÁTICA EN ECOSISTEMAS IOT POR MEDIO DE UN HONEYPOT QUE SIMULE UN DISPOSITIVO INTELIGENTE PARA ALERTAR Y PREVENIR ATAQUES EN LA RED"

**AUTOR:** BRYAN ANDRÉS HERNÁNDEZ CUEVA

**DIRECTOR:** ING. DARWIN OMAR ALULEMA FLORES, PhD.

**QUITO-ECUADOR**
**2023**

**VERSIÓN:** 1.1

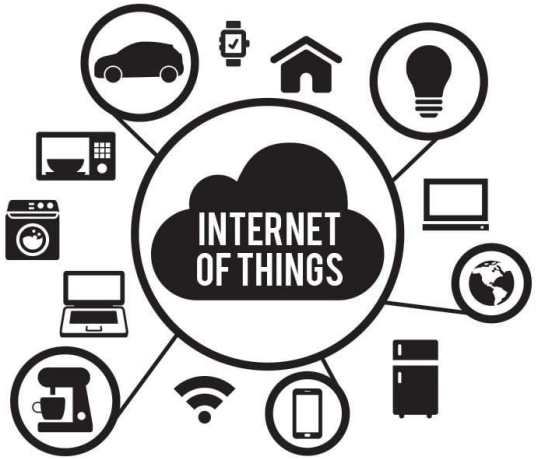
# AGENDA

1. Introducción
2. Objetivos
3. Marco Conceptual
4. Diseño
5. Implementación
6. Pruebas y Resultados
7. Conclusiones y Recomendaciones
8. Trabajos Futuros

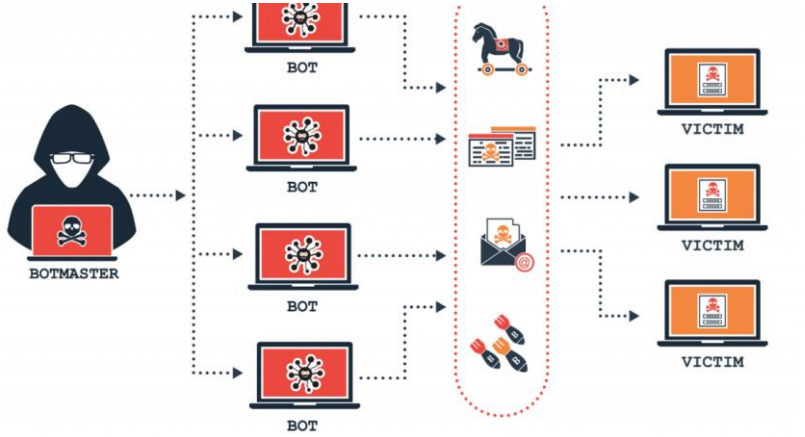
# INTRODUCCIÓN

## Antecedentes

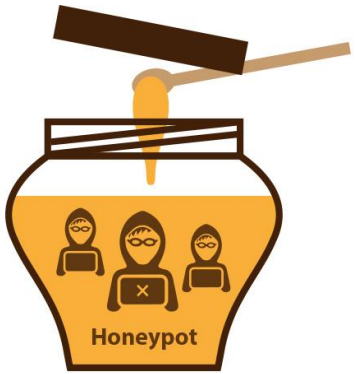
Amenazas informáticas




Internet de las cosas (IoT)




Botnets

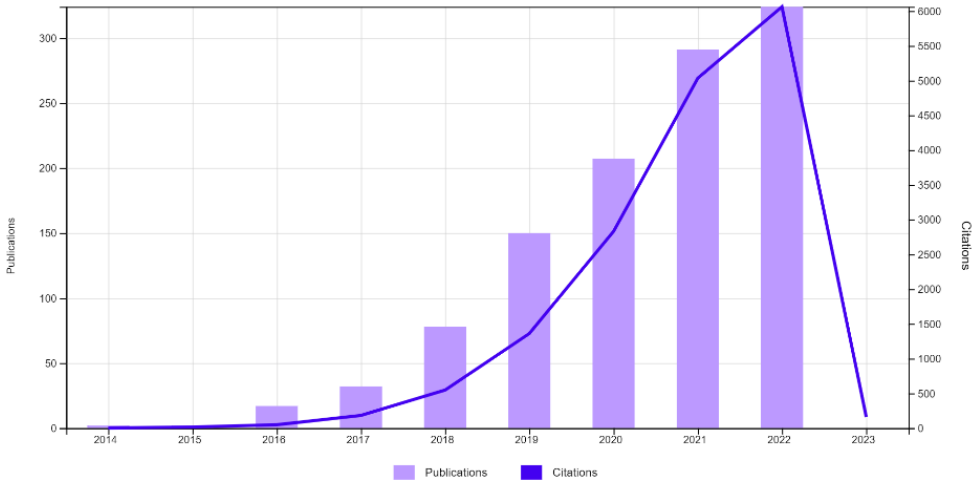


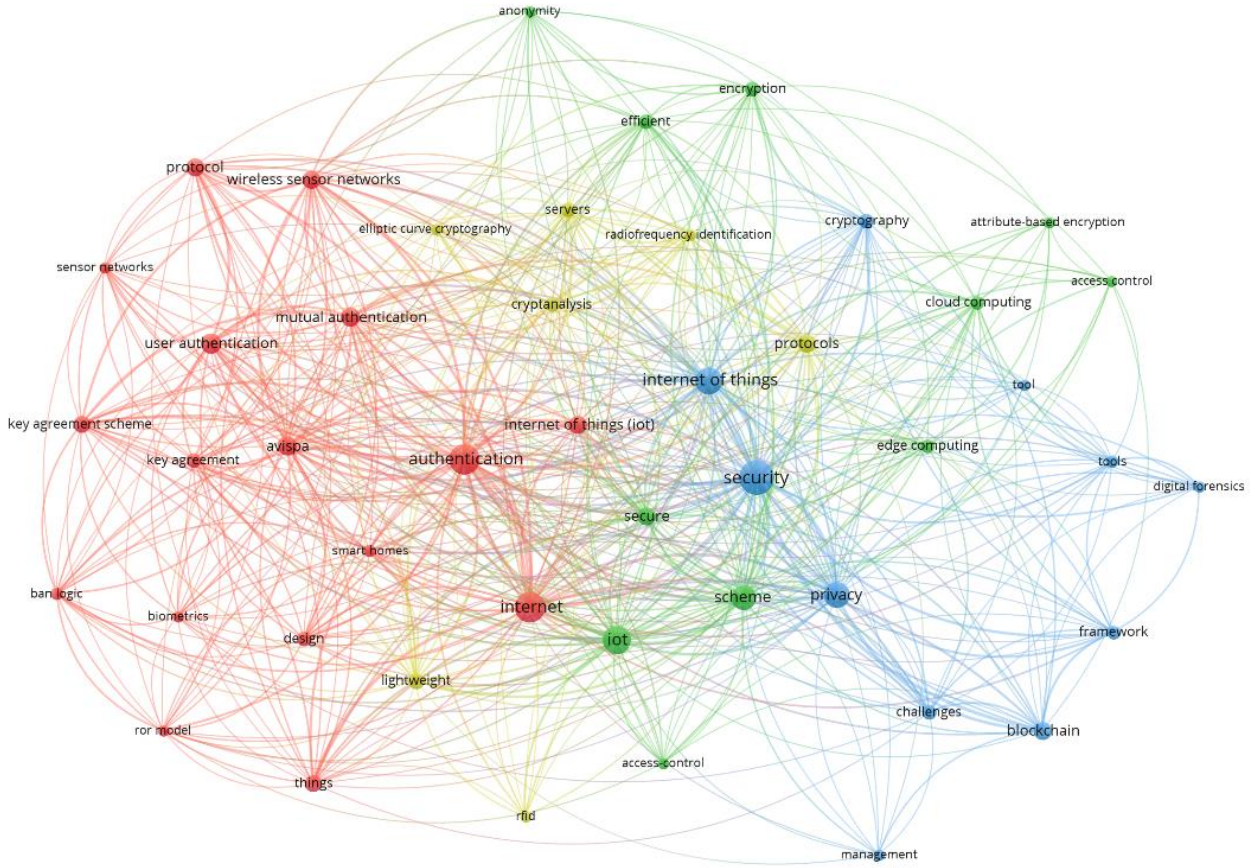

Honeypot

# INTRODUCCIÓN

## Estado del Arte

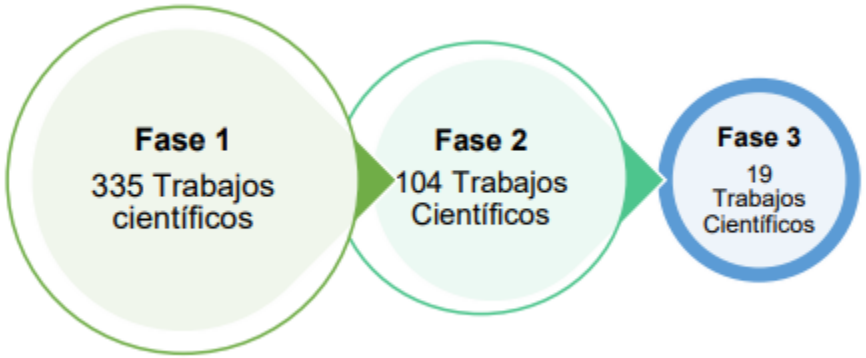

## Mapeo Sistemático de la Literatura (SMS)



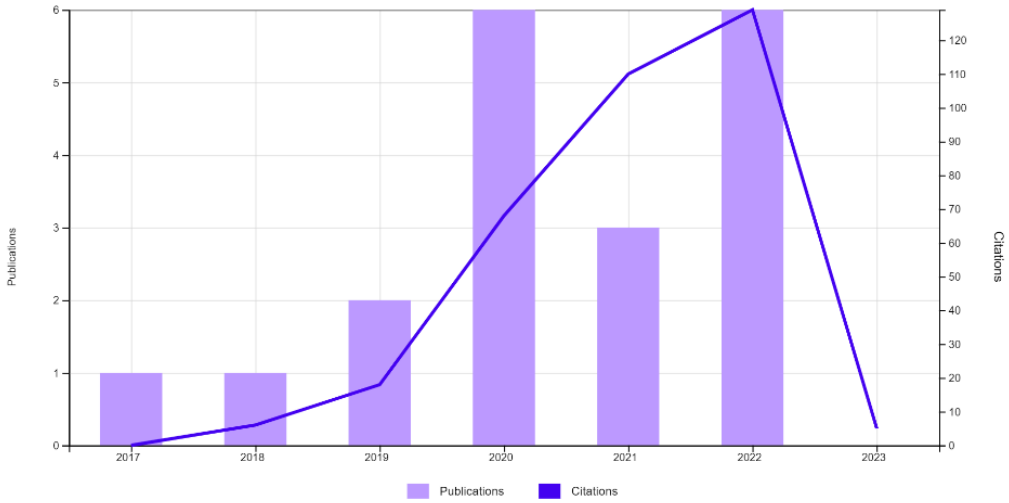



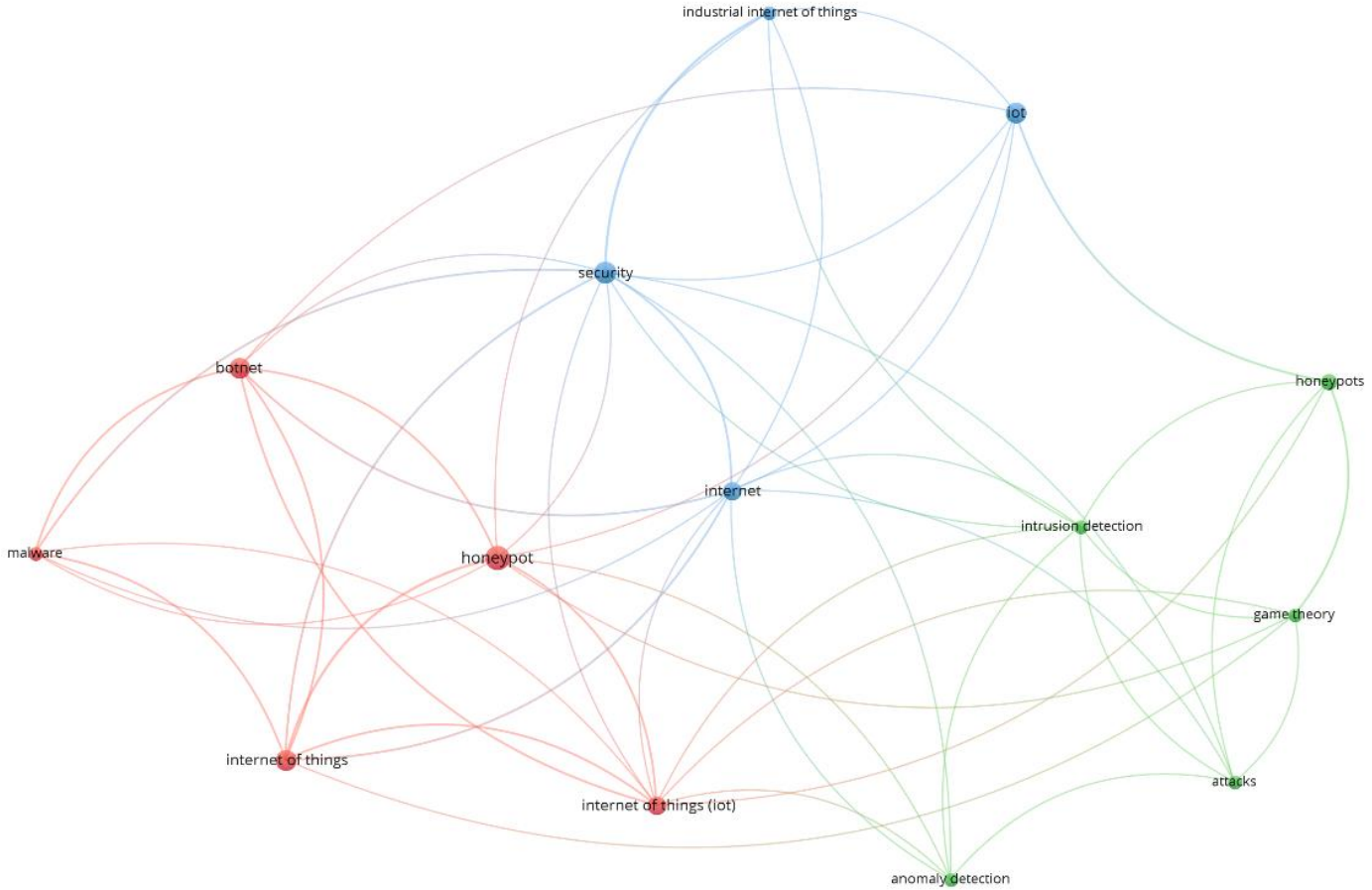
# INTRODUCCIÓN

## Estado del Arte



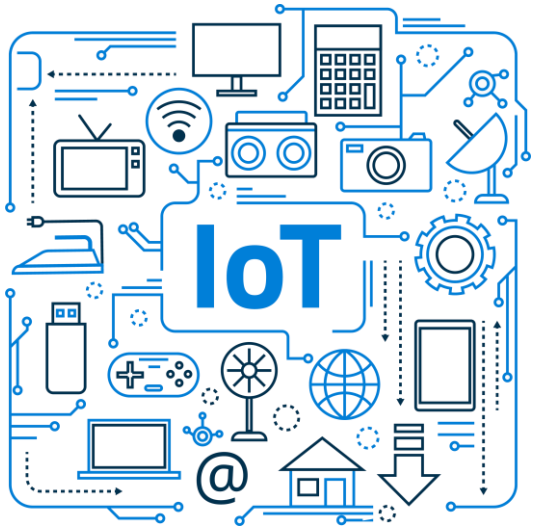

Revisión Sistemática de la Literatura (SLR)



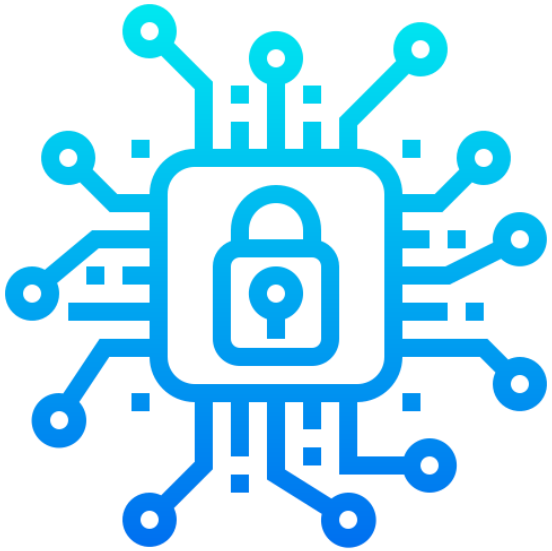
# INTRODUCCIÓN

## Alcance




Entornos IoT


Granja de Honeypots



Solución de Seguridad Informática

# OBJETIVOS

## Objetivo General

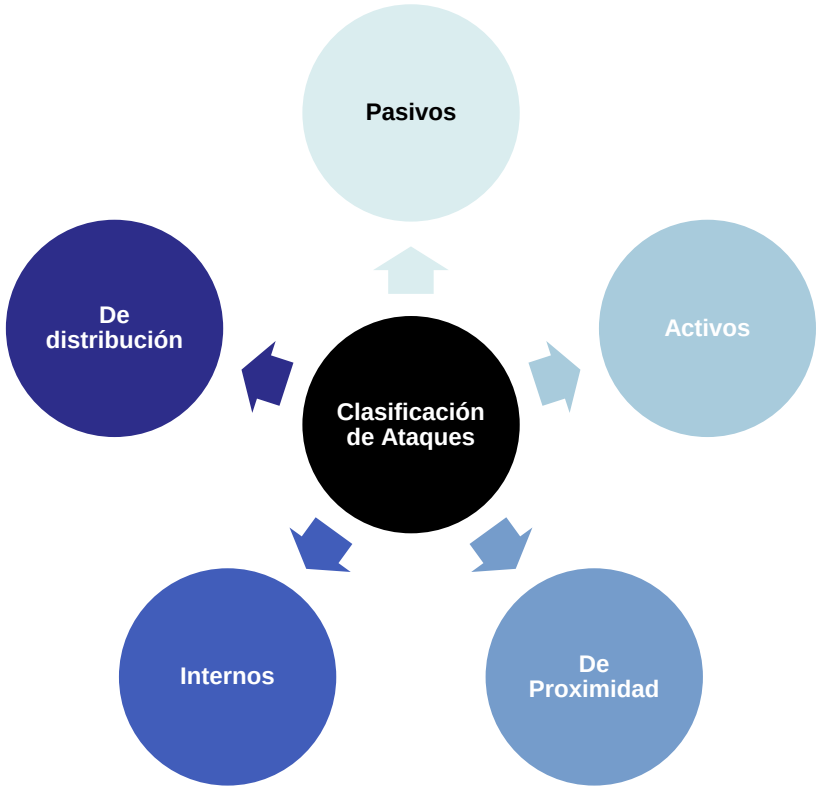
Evaluar las vulnerabilidades de seguridad informática dentro de entornos del Internet de las Cosas a través de una Honeynet híbrida para alertar y prevenir ataques a la red.

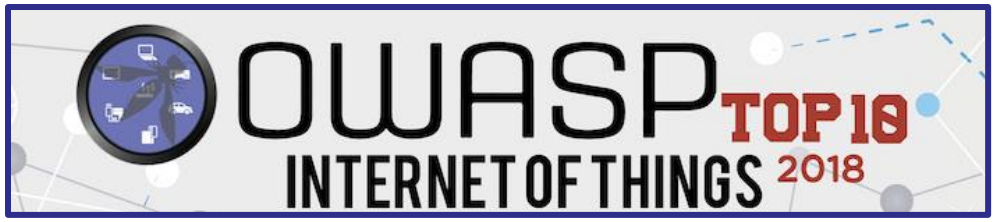
## Objetivos Especificos

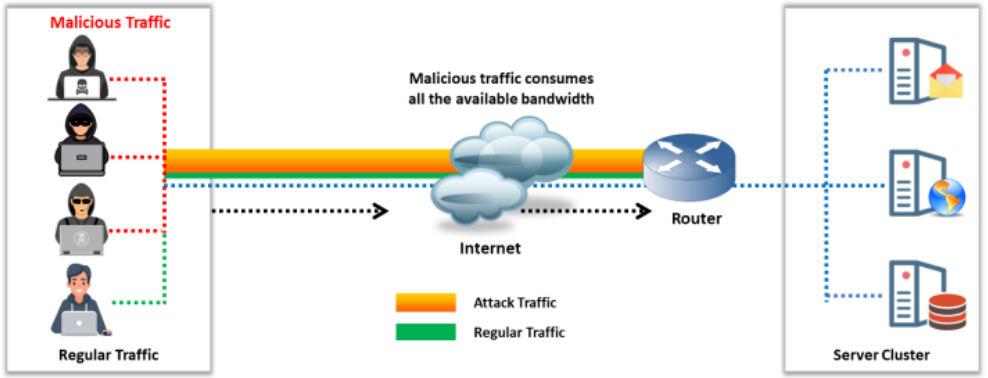
- Investigar normativa y recomendaciones enfocadas a la ciberseguridad de redes y dispositivos del Internet de las Cosas.
- Identificar los principales problemas de seguridad informática ligados con el Internet de las Cosas.
- Desplegar un escenario de prueba donde la Honeynet híbrida sea capaz de detectar y recoger información de ataques dirigidos a entornos IoT.
- Implementar un honeypot físico a través de una Raspberry Pi y dos honeypots virtuales que finjan ser servidores de producción dentro de una red IoT para ser objetos de posibles irrupciones.
- Analizar los resultados obtenidos con la integración de la Honeynet híbrida dentro de un ecosistema del Internet de las Cosas.

# MARCO CONCEPTUAL

Vulnerabilidad → Amenaza → Exploit

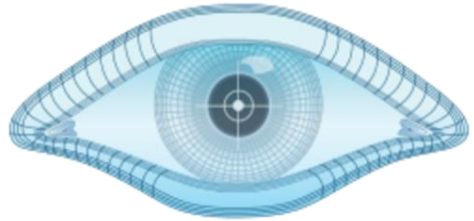



# MARCO CONCEPTUAL

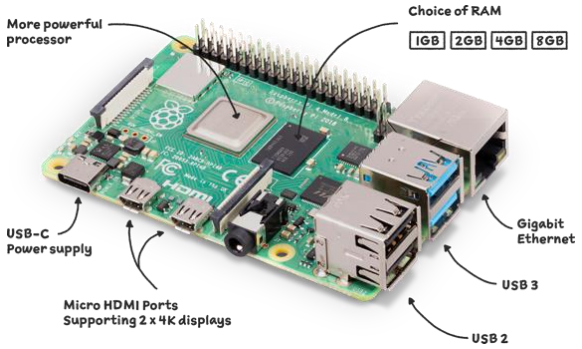




NMAP

## Honeypot

| | | | | |
|---|---|---|---|---|
| Producción | Investigación | Baja Interacción | Alta Interacción | Interacción media |



# DISEÑO

## Directrices de Seguridad

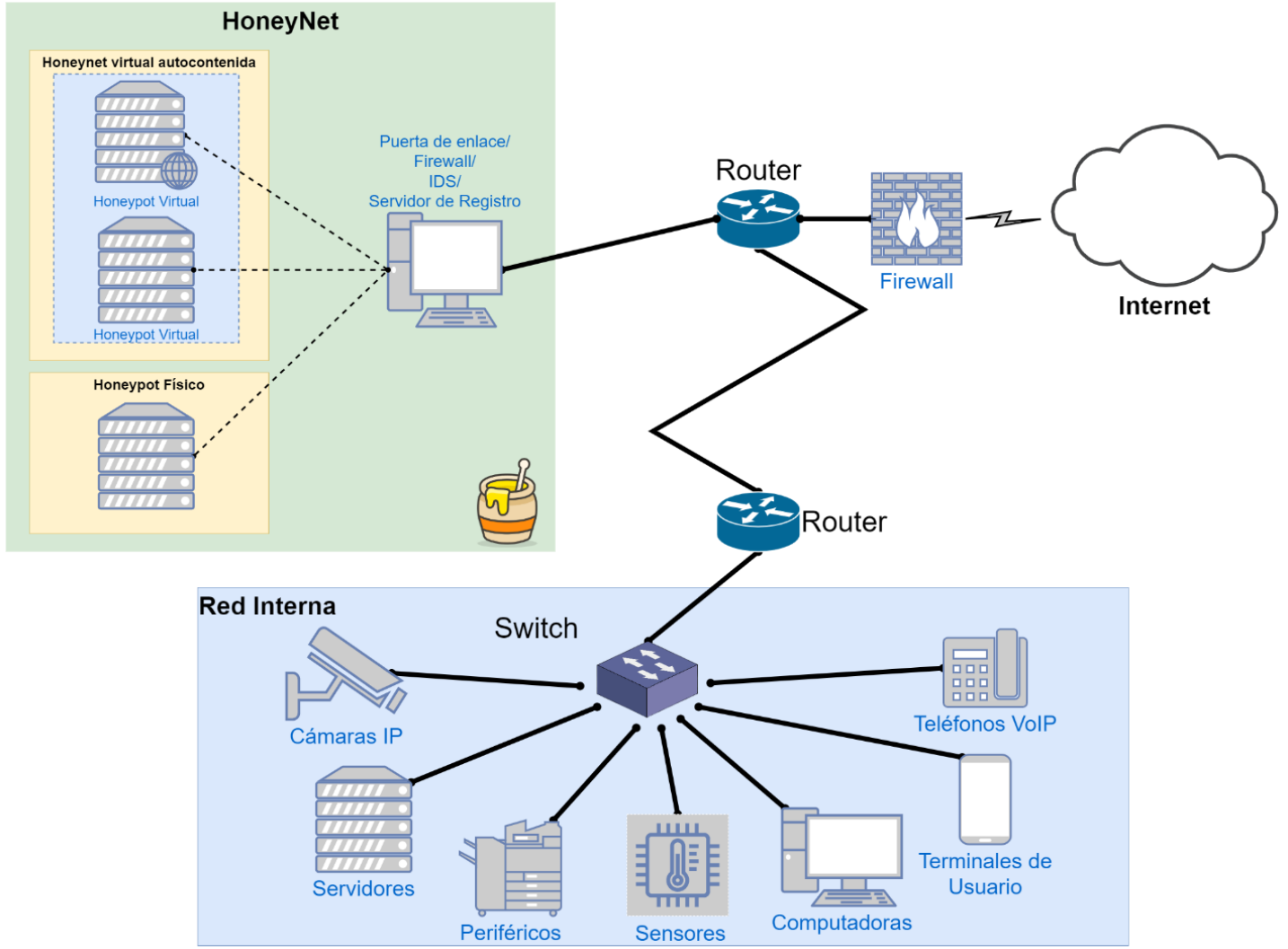
- Orientaciones generales
  - Comunicación segura: Los honeypots cifran todos los datos y se envían a la Honeynet.
  - Autenticación de dispositivos: La honeynet maneja una clave única para identificar los sensores desplegados y conectados dentro de la solución.
  - Capacidad de auditoría: El servidor de registros MHN recolecta toda la información captada por los sensores.
  - Integración segura: El servidor MHN permite integrarse con otras herramientas de seguridad para monitorear los eventos en la red como un SIEM.
  - Gestión de identidades: Dentro del servidor de registros se puede configurar y agregar nuevos usuarios para administrar el mismo. Adicionalmente los routers utilizados dentro de la arquitectura permiten la creación de cuentas de usuarios con diferentes perfiles para la administración y configuración de los diferentes parámetros del dispositivo.
  - Análisis de vulnerabilidades: El MHN analiza y cataloga las vulnerabilidades conocidas registradas por cada sistema trampa.

# DISEÑO

## Directrices de Seguridad

- Orientaciones de seguridad de pasarelas
  - Detección de intrusos: El MHN cumple las funciones de una herramienta de detección de intrusos (IDS).
  - Control de Acceso: Solo los usuarios con las credenciales de administrador pueden acceder a los diferentes elementos de red y a la información almacenada en los registros de eventos.
- Orientaciones de seguridad en la red
  - Perímetro de seguridad física
  - Seguridad en instalaciones
  - Protección contra las amenazas ambientales y externas: Los servidores de la solución de seguridad no se encuentran desplegados en un ambiente hostil. Mientras tanto la solución IoT por su naturaleza está únicamente expuesta a un entorno previamente estudiado.
  - Seguridad del cableado
  - Protección contra eliminación de activos: El servidor MHN al igual que cada uno de los servidores que contienen los honeypots se encuentran debidamente configurados para impedir el acceso a personal no autorizado.
  - Controles de red
  - Segmentación en las redes

# DISEÑO


HoneyNet
Honeynet virtual autocontenida
Honeypot Virtual
Honeypot Virtual
Honeypot Físico
Puerta de enlace/
Firewall/
IDS/
Servidor de Registro
Router
Firewall
Internet
Router
Red Interna
Switch
Cámaras IP
Teléfonos VoIP
Servidores
Periféricos
Sensores
Computadoras
Terminales de
Usuario

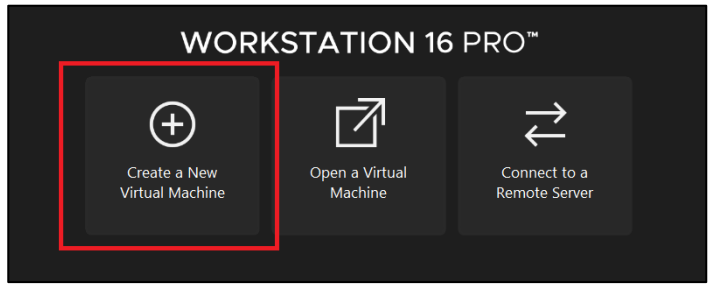
# IMPLEMENTACIÓN

| Cantidad | Elemento de red | Descripción |
|---|---|---|
| **1** | Raspberry Pi | Es un ordenador de bajo costo el cual alojará un honeypot físico.<br>Características:<br>• RAM: 2 GB<br>• Procesador: Broadcom BCM2711 |
| **1** | Computador Asus | Computador con altas capacidades para el alojamiento de parte de la honeynet así como el servidor de registro.<br><br>Características:<br>• RAM: 16 GB<br>• Almacenamiento: 512 GB Estado Sólido.<br>• Sistema Operativo: Windows 10<br>• Procesador: Intel Core i7 |
| **1** | Optical Network Terminal | Es el router que generalmente el ISP entrega al momento de la instalación de un servicio de Internet por fibra óptica. |
| **1** | Router Inalámbrico | Se seleccionó uno de acuerdo a las necesidades de cobertura de la red IoT y dependerá también de la frecuencia que trabajen los elementos de red a los que de servicio. |

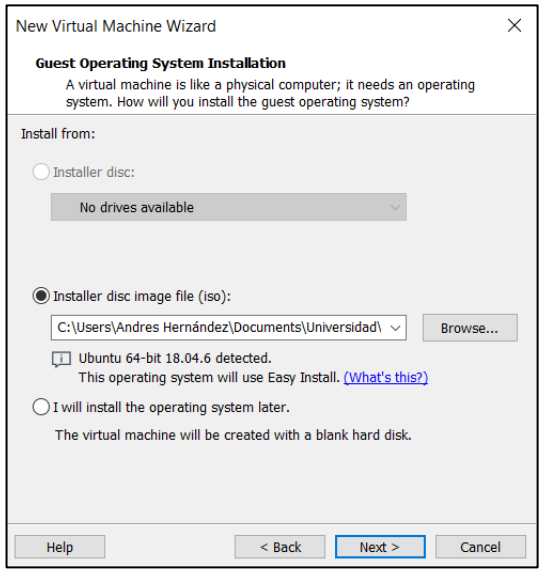
# IMPLEMENTACIÓN

## Configuración de las MVs

1

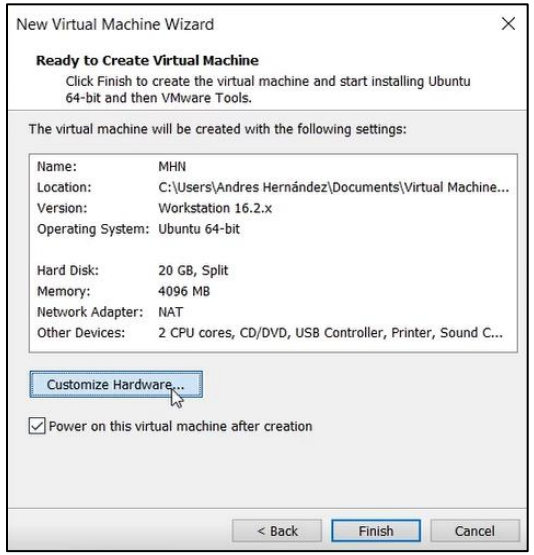



2

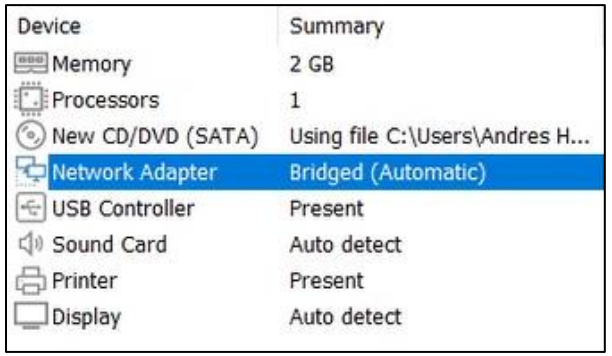



3


4




5



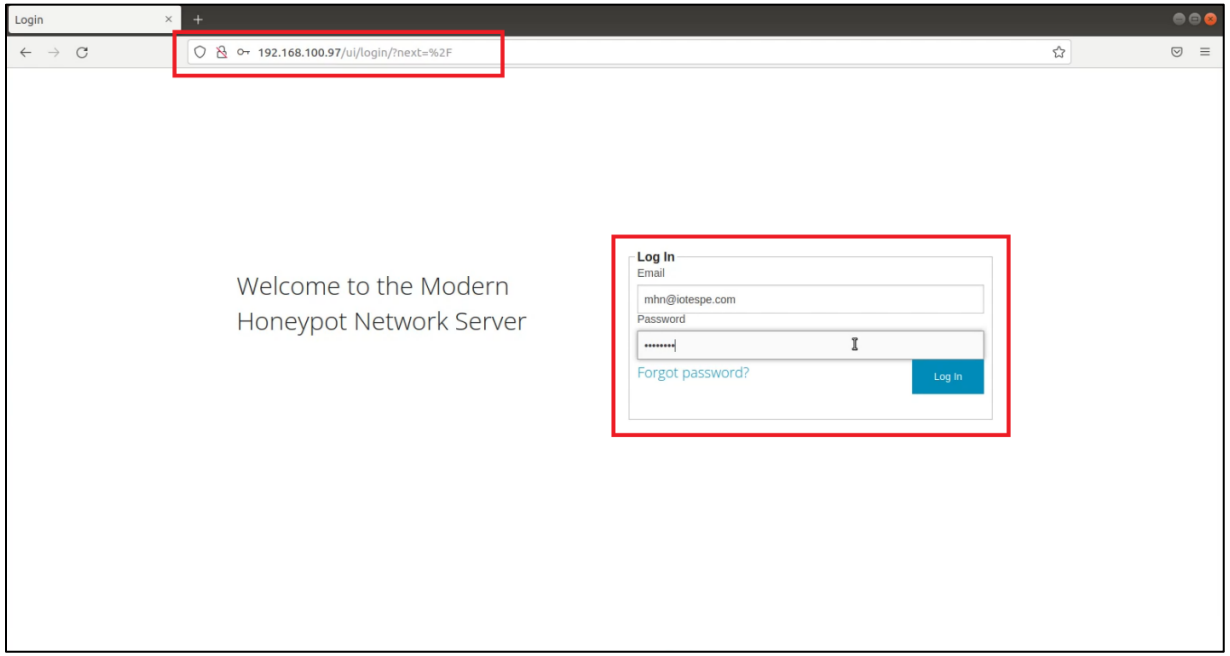
# IMPLEMENTACIÓN

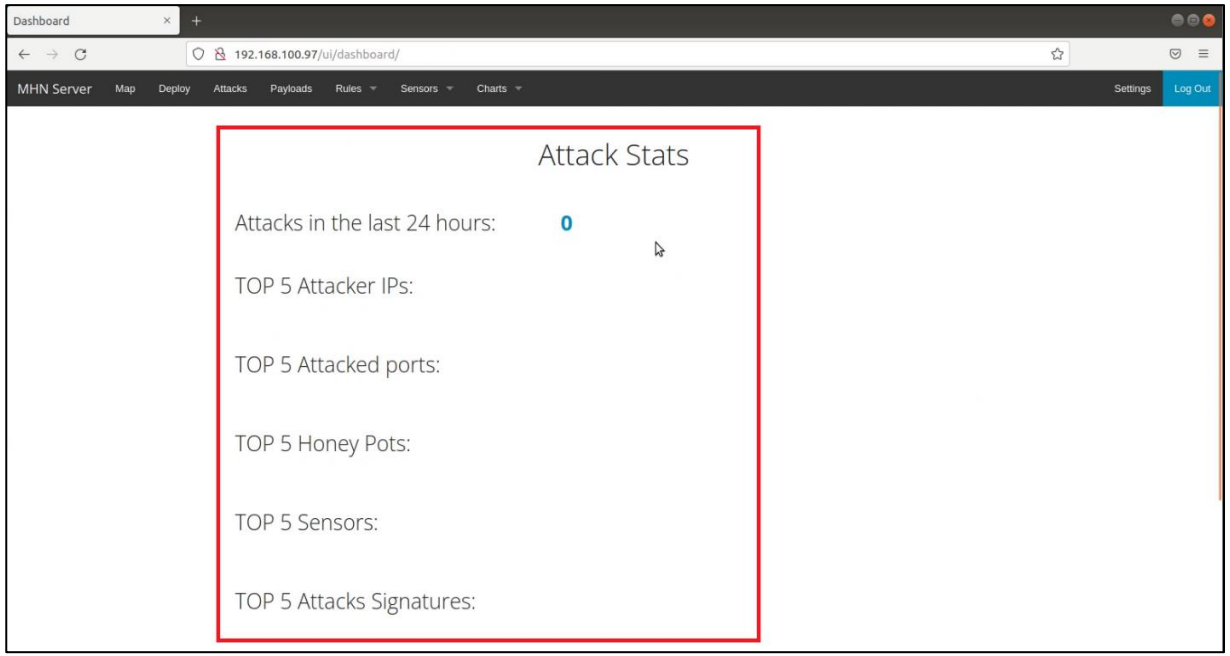
## Modern Honey Network

- Permite la implementación de diferentes señuelos de forma rápida.
- Configura automáticamente la conexión entre servidor de administración y sistema trampa.
- Cuenta con diferentes tecnologías de honeypot, incluyendo las más comunes.
- Posee una interfaz gráfica web.
- Existe una comunidad que constantemente está resolviendo posibles fallos de la solución.
- Software de código abierto.
- Existe amplia documentación sobre la herramienta.
- Permite la integración con herramientas de seguridad como el SIEM.
- Cuenta con un gran catálogo de reglas de seguridad definidas de manera nativa.
- Recopila toda la información de los diferentes sensores implementados.
- Almacena toda la data de manera sigilosa, centralizada y automáticamente

# IMPLEMENTACIÓN

## Modern Honey Network

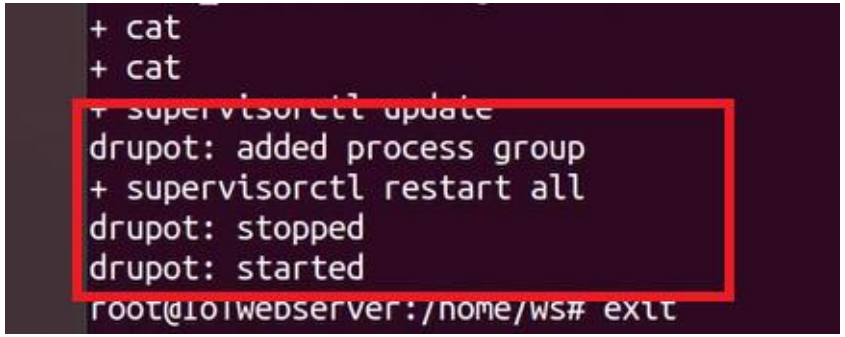


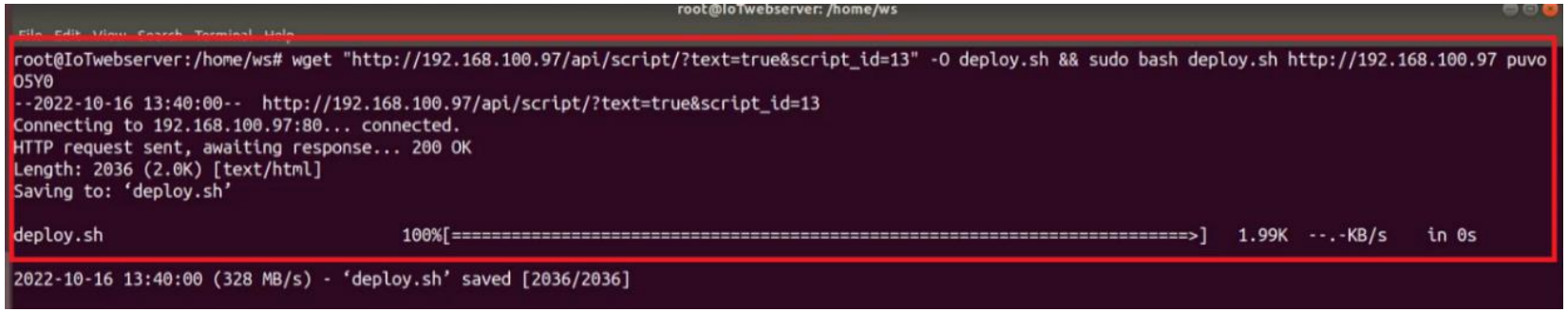



# IMPLEMENTACIÓN

## Drupot

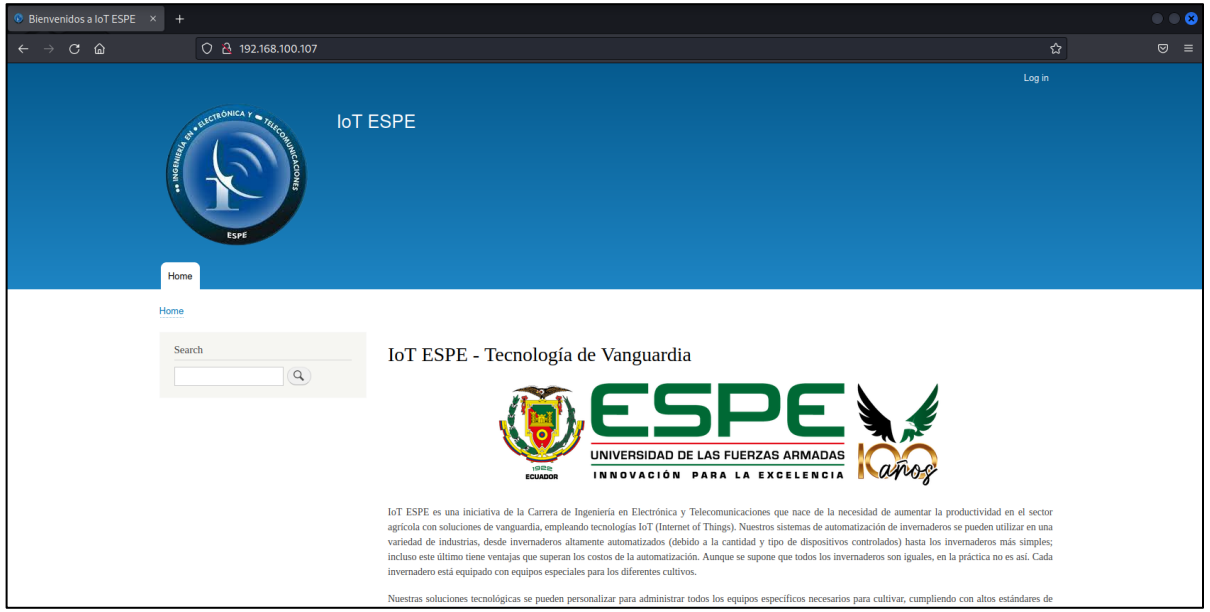
- Honeypot de interacción media.
- Emula servicios web.
- Posee una interfaz web atractiva.
- Permite detectar ataques de inyección de código.
- Registra todas las conexiones entrantes al sistema.
- Bloquea a los robots de spam.
- Fácil configuración e integración dentro de una arquitectura de red.
- Existen manuales disponibles para su correcta configuración.
- Fácil administración y mantenimiento.

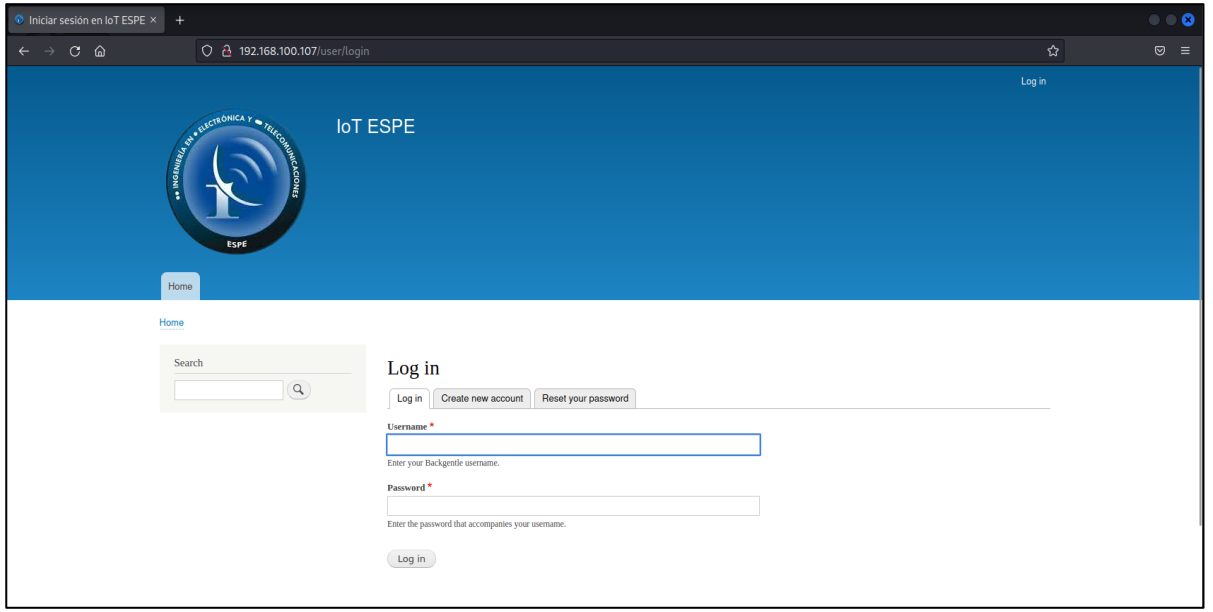


# IMPLEMENTACIÓN

## Drupot

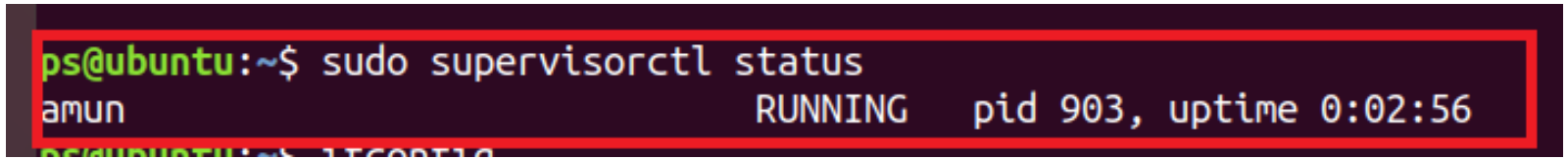


# IMPLEMENTACIÓN

## Amun

- Honeypot de interacción baja.
- Emula servicios atractivos como ftp, telnet, smtp, entre otros.
- Desarrollado en Python.
- Permite registrar malware de propagación automática.
- Fácil instalación y configuración.
- Fácil administración y mantenimiento.
- Cataloga toda la información registrada en diferentes módulos.
- Proporciona información detallada del ataque.



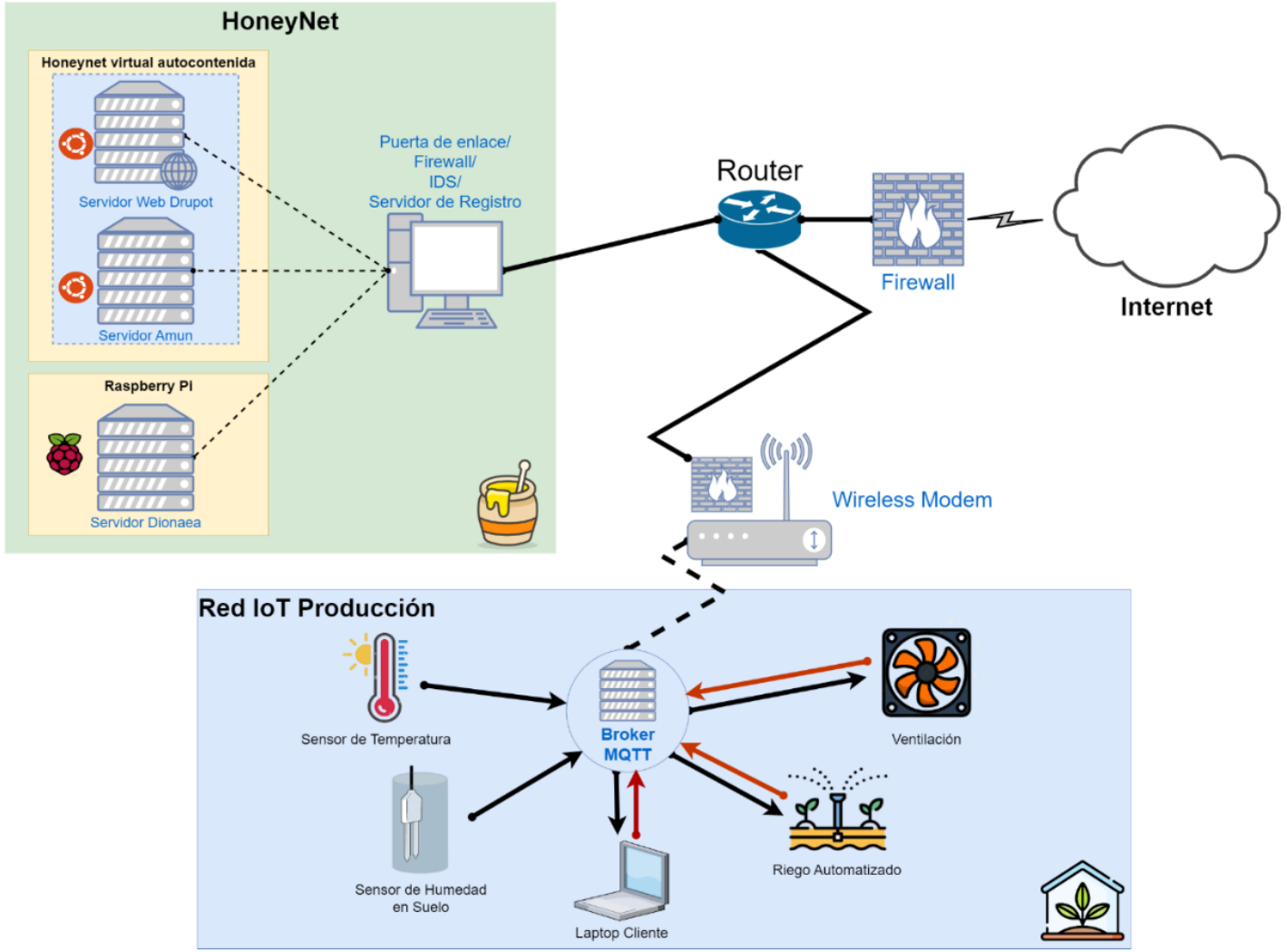
# IMPLEMENTACIÓN

## Dionaea

- Honeypot de interacción baja.
- Diseñado para atrapar malware dirigido a servicios de red.
- Publica servicios como FTP, SMB, Base de Datos, MQTT, etc.
- Soporta rutinas no bloqueantes.
- Fácil instalación y configuración.
- Fácil administración y mantenimiento.
- Permite levantar diferentes módulos y servicios vulnerables.
- Guarda una copia de los shellcodes y registra los métodos utilizados por el atacante durante la fase de explotación.

```
pi@IoTDBserver:~ $ sudo supervisorctl status
sudo: unable to resolve host IoTDBserver: Nombre o servicio desconocido
dionaea                          RUNNING   pid 971, uptime 20 days, 13:17:11
```

# IMPLEMENTACIÓN



# PRUEBAS

## Máquina Atacante

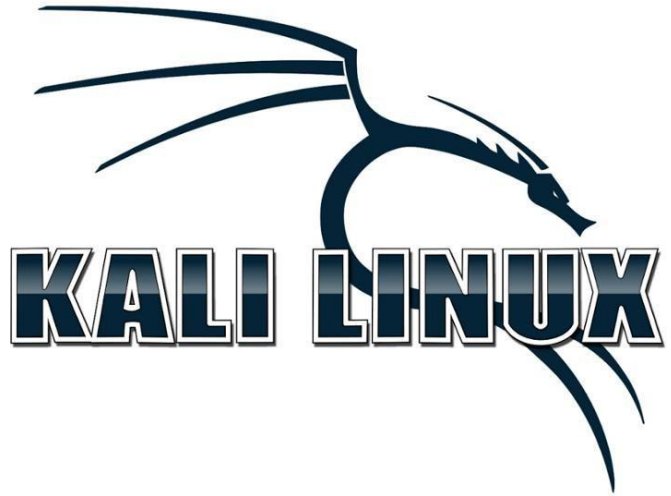
Para atacar la red se utilizó una máquina virtual Kali Linux la cual se encuentra en el mismo segmento de red que la Honeynet Híbrida y del AP (Access Point) del ecosistema IoT.

Especificaciones técnicas

- **Software de virtualización:** Se utilizó VMware Workstation 16.2.4
- **Procesadores:** 4 núcleos
- **RAM:** 4 GB
- **Adaptador de red:** Bridged

Datos de Red

- **IPv4:** 192.168.100.100
- **Máscara:** 255.255.255.0



# PRUEBAS

## Escaneo de red

Se realiza un escaneo ARP para identificar los equipos dentro de la red con el comando arp-scan y parámetro -l. A partir de este punto se utilizará niveles de superusuario para tener acceso completo a las herramientas.

```
┌──(root㉿kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:16:1d:65, IPv4: 192.168.100.100
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.100.1                           HUAWEI TECHNOLOGIES CO.,LTD
192.168.100.1                           HUAWEI TECHNOLOGIES CO.,LTD (DUP: 2)
192.168.100.6                           ASUSTek COMPUTER INC.
192.168.100.79                          (Unknown)
192.168.100.88                          (Unknown)
192.168.100.97  00:0c:29:b5:9c:c7       VMware, Inc.
192.168.100.107 00:0c:29:3b:cb:b4       VMware, Inc.
192.168.100.108 00:0c:29:b7:80:80       VMware, Inc.

15 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.971 seconds (129.88 hosts/sec). 8 responded
```



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# PRUEBAS

## Escaneo de puertos y sistemas operativos

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -Pn -p- 192.168.100.79
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-23 19:00 EDT
Nmap scan report for 192.168.100.79
Host is up (0.00093s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
1723/tcp  open  pptp
1883/tcp  open  mqtt
3306/tcp  open  mysql
5060/tcp  open  sip
5061/tcp  open  sip-tls
11211/tcp open  memcache
27017/tcp open  mongod
MAC Address:                  (Raspberry Pi Trading)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.18 seconds
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O -Pn -p- 192.168.100.107
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-04 19:38 EDT
Nmap scan report for 192.168.100.107
Host is up (0.00057s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:3B:CB:B4 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.74 seconds
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O -Pn -p- 192.168.100.108
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-04 19:44 EDT
Nmap scan report for 192.168.100.108
Host is up (0.00071s latency).
Not shown: 65484 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
80/tcp    open  http
105/tcp   open  csnet-ns
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
587/tcp   open  submission
617/tcp   open  sco-dtmgr
1023/tcp  open  netvenuechat
1025/tcp  open  NFS-or-IIS
1080/tcp  open  socks
1111/tcp  open  lmsocialserver
1581/tcp  open  mil-2045-47001
1900/tcp  open  upnp
2101/tcp  open  rtcm-sc104
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
2380/tcp  open  etcd-server
2555/tcp  open  compaq-wcp
2745/tcp  open  urbisnet
2954/tcp  open  ovalarmsrv-cmd
2967/tcp  open  symantec-av
2968/tcp  open  enpp
3127/tcp  open  ctx-bridge
3128/tcp  open  squid-http
3268/tcp  open  globalcatLDAP
3372/tcp  open  msdtc
3389/tcp  open  ms-wbt-server
3628/tcp  open  ept-machine
5000/tcp  open  upnp
5168/tcp  open  scte30
5554/tcp  open  sgi-esphttp
6070/tcp  open  messageasap
6101/tcp  open  backupexec
6129/tcp  open  unknown
7144/tcp  open  unknown
7547/tcp  open  cwmp
8080/tcp  open  http-proxy
9999/tcp  open  abyss
10203/tcp open  unknown
27347/tcp open  unknown
38292/tcp open  landesk-cba
41523/tcp open  unknown
MAC Address: 00:0C:29:B7:80:80 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:lir
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect
Nmap done: 1 IP address (1 host up) scanned in 3.87
```



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# PRUEBAS

## Puerto 21

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ftp 192.168.100.79
Connected to 192.168.100.79.
220 DiskStation FTP server ready.
Name (192.168.100.79:kali): anonymous
331 Guest login ok, type your email address as password.
Password:
230 Anonymous login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.100.108
Connected to 192.168.100.108.
220 Welcome to my FTP Server
Name (192.168.100.108:kali): anonymous
331 User OK, Password required
Password:
230 User logged in, proceed
ftp> ls
500 Unknown Command.
500 Unknown Command.
ftp: Can't bind for data connection: Address already in use
ftp> dir
500 Unknown Command.
```

## Puerto 80

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p80 -A 192.168.100.107
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-05 18:23 EDT
Nmap scan report for 192.168.100.107
Host is up (0.00076s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Date: Sat, 05 Nov 2022 22:23:11 GMT
|     Content-Type: text/html; charset=utf-8
|     <!DOCTYPE html>
|     <html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/mod
p.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# schema: http://schema.o
org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema# ">
|     <head>
|     <meta charset="utf-8" />
|     <meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
|     <meta name="MobileOptimized" content="width" />
|     <meta name="HandheldFriendly" content="true" />
|     <meta name="viewport" content="width=device-width, initial-scale=1.0"
|     <link rel="shortcut icon" href="/core/misc/favicon1.ico" type="image/v
|     <link rel="alterna
|_http-title: Bienvenidos a IoT ESPE
|_http-generator: Drupal 8 (https://www.drupal.org)
1 service unrecognized despite returning data. If you know the service/versi
MAC Address: 00:0C:29:3B:CB:B4 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.76 ms 192.168.100.107

OS and Service detection performed. Please report any incorrect results at h
Nmap done: 1 IP address (1 host up) scanned in 88.46 seconds
```



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# PRUEBAS

## Puerto 445

Este puerto es uno de los más usuales y fácilmente propensos para ataques informáticos. El mismo al ser un puerto TCP permite compartir archivos SMB de Microsoft-DS.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -p 445 -A 192.168.100.79
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-04 20:12 EDT
Nmap scan report for 192.168.100.79
Host is up (0.00070s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Windows XP microsoft-ds
MAC Address:                  (Raspberry Pi Trading)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

Host script results:
|_clock-skew: mean: -36m16s, deviation: 42m24s, median: -1h06m16s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   NetBIOS computer name: HOMEUSER-3AF6FE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-11-05T01:06:25+01:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms 192.168.100.79

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap --script smb-vuln* -p 445 192.168.100.79
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-04 20:18 EDT
Nmap scan report for 192.168.100.79
Host is up (0.0010s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address:                  (Raspberry Pi Trading)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 23.91 seconds
```



UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# PRUEBAS

## Puerto 1883

Este es el puerto predeterminado para el protocolo de mensajería/suscripción MQTT. Como se observa el servidor A cuenta con este puerto abierto, por lo que se procederá a explotarlo. Para esto se realizará un ataque de fuerza bruta, debido a que en el protocolo MQTT la autenticación es opcional y a pesar de que se implementen las credenciales, estas no son cifradas y se envían en texto claro.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -p 1883 --script mqtt-subscribe 192.168.100.79
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-04 22:05 EDT
Nmap scan report for 192.168.100.79
Host is up (0.0031s latency).

PORT     STATE SERVICE
1883/tcp open  mqtt
|_mqtt-subscribe: Every topic filter was rejected.
MAC Address:                    (Raspberry Pi Trading)

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

```
msf6 > use auxiliary/scanner/mqtt/connect
msf6 auxiliary(scanner/mqtt/connect) > set PASS_FILE /tmp/passwords.txt
PASS_FILE ⇒ /tmp/passwords.txt
msf6 auxiliary(scanner/mqtt/connect) > set USER_FILE /tmp/users.txt
USER_FILE ⇒ /tmp/users.txt
msf6 auxiliary(scanner/mqtt/connect) > set rhosts 192.168.100.79
rhosts ⇒ 192.168.100.79
msf6 auxiliary(scanner/mqtt/connect) > show options

Module options (auxiliary/scanner/mqtt/connect):

   Name              Current Setting     Required  Description
   ----              ---------------     --------  -----------
   BLANK_PASSWORDS   false               no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                   yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false               no        Try each user/password couple stored in the current
   DB_ALL_PASS       false               no        Add all passwords in the current database to the lis
   DB_ALL_USERS      false               no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                no        Skip existing credentials stored in the current data
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE         /tmp/passwords.txt  no        File containing passwords, one per line
   RHOSTS            192.168.100.79      yes       The target host(s), see https://github.com/rapid7/m
   RPORT             1883                yes       The target port (TCP)
   STOP_ON_SUCCESS   false               yes       Stop guessing when a credential works for a host
   THREADS           1                   yes       The number of concurrent threads (max one per host)
   USERNAME                              no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by spa
   USER_AS_PASS      true                no        Try the username as the password for all users
   USER_FILE         /tmp/users.txt      no        File containing usernames, one per line
   VERBOSE           true                yes       Whether to print output for all attempts

msf6 auxiliary(scanner/mqtt/connect) > exploit

[-] 192.168.100.79:1883   - Msf::OptionValidateError The following options failed to validate: USER_FILE, PASS_FILE
```



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# PRUEBAS

## Puerto 3306

MySQL es un sistema de gestión de base de datos relacional, el mismo que corre sobre el puerto 3306 por defecto, en el servidor A este puerto se encuentra abierto por lo que se pudo observar en la primera fase de recopilación activa de información, ahora nuevamente con la ayuda de la herramienta Nmap se escaneara solo el puerto 3306 para descubrir más información solo de este puerto y verificar si el mismo es explotable.

```
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.7.16
| mysql-info:
|   Protocol: 10
|   Version: 5.7.16
|   Thread ID: 1729232896
|   Capabilities flags: 41516
|   Some Capabilities: Support41Auth, SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: aaaaaaaa
MAC Address:                 (Raspberry Pi Trading)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap --script=mysql-brute 192.168.100.79
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-05 13:37 EDT
Nmap scan report for 192.168.100.79
Host is up (0.0017s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
1723/tcp open  pptp
3306/tcp open  mysql
| mysql-brute:
|   Accounts:
|     administrator:administrator - Valid credentials
|     netadmin:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     test:test - Valid credentials
|     sysadmin:sysadmin - Valid credentials
|     root:root - Valid credentials
|     admin:admin - Valid credentials
|     webadmin:webadmin - Valid credentials
|     web:web - Valid credentials
|_  Statistics: Performed 26 guesses in 2 seconds, average tps: 13.0
5060/tcp open  sip
5061/tcp open  sip-tls
MAC Address:                   (Raspberry Pi Trading)

Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# RESULTADOS

## Pruebas de funcionamiento del Honeypot Dionaea

Attacks Report

Search Filters

| Sensor | Honeypot | Date | Port | IP Address | |
|---|---|---|---|---|---|
| IoTDBserver | All | MM-DD-YYYY | 21 | 8.8.8.8 | GO |

| | Date | Sensor | Country | Src IP | Dst port | Protocol | Honeypot |
|---|---|---|---|---|---|---|---|
| 1 | 2022-11-05 00:04:30 | IoTDBserver | | 192.168.100.100 | 21 | ftpd | dionaea |
| 2 | 2022-11-05 00:02:13 | IoTDBserver | | 192.168.100.100 | 21 | ftpd | dionaea |

Attacks Report

Search Filters

| Sensor | Honeypot | Date | Port | IP Address | |
|---|---|---|---|---|---|
| IoTDBserver | All | MM-DD-YYYY | 445 | 8.8.8.8 | GO |

| | Date | Sensor | Country | Src IP | Dst port | Protocol | Honeypot |
|---|---|---|---|---|---|---|---|
| 1 | 2022-11-05 00:21:21 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |
| 2 | 2022-11-05 00:18:08 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |
| 3 | 2022-11-05 00:18:03 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |
| 4 | 2022-11-05 00:12:46 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |
| 5 | 2022-11-05 00:12:45 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |
| 6 | 2022-11-05 00:12:44 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |
| 7 | 2022-11-05 00:12:43 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |
| 8 | 2022-11-05 00:12:43 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |
| 9 | 2022-11-05 00:12:42 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |
| 10 | 2022-11-05 00:12:41 | IoTDBserver | | 192.168.100.100 | 445 | smbd | dionaea |

1 2 »

```
pi@IoTDBserver:/opt/dionaea/var/lib/dionaea/bistreams/2022-11-04 $ ls
epmapper-192.168.100.79-135-192.168.100.100-35037-2022-11-05T00:10:05.653120-NwLs0i
ftpd-192.168.100.79-21-192.168.100.100-45596-2022-11-05T00:02:05.795056-zMUkdT
mqttd-192.168.100.79-1883-192.168.100.100-37132-2022-11-05T02:35:05.394488-CtKIRP
mqttd-192.168.100.79-1883-192.168.100.100-42840-2022-11-05T02:03:05.905751-FuwXoP
mqttd-192.168.100.79-1883-192.168.100.100-50696-2022-11-05T02:05:05.061868-lkM0lU
mqttd-192.168.100.79-1883-192.168.100.100-53510-2022-11-05T02:03:05.553050-lrEKOK
mqttd-192.168.100.79-1883-192.168.100.100-59578-2022-11-05T02:35:05.771512-c24qxL
smbd-192.168.100.79-445-192.168.100.100-34247-2022-11-05T00:21:05.545880-CoDVR4
smbd-192.168.100.79-445-192.168.100.100-34554-2022-11-05T00:18:05.362644-IhCVkp
smbd-192.168.100.79-445-192.168.100.100-35214-2022-11-05T00:18:05.387131-dXr9rn
smbd-192.168.100.79-445-192.168.100.100-35216-2022-11-05T00:18:05.577909-V4c467
smbd-192.168.100.79-445-192.168.100.100-35218-2022-11-05T00:18:05.778547-dzOc06
smbd-192.168.100.79-445-192.168.100.100-35232-2022-11-05T00:18:05.993160-mVyMMa
```

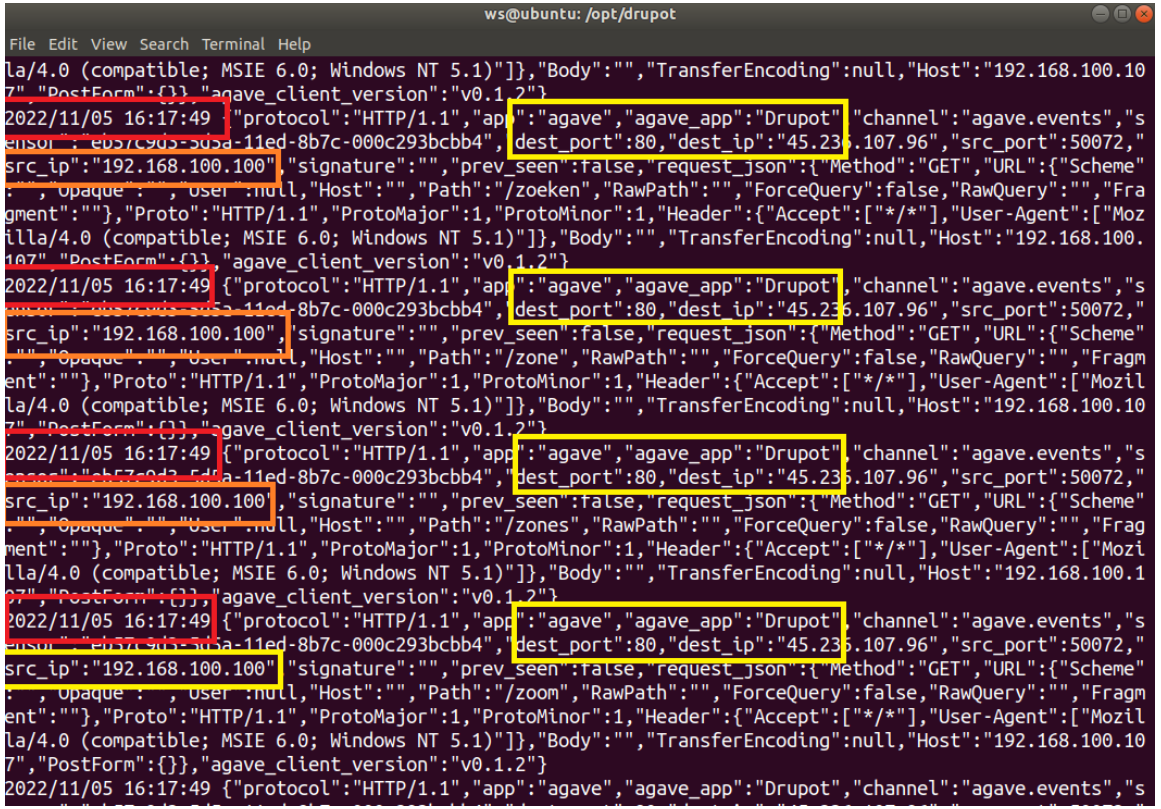


ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# RESULTADOS

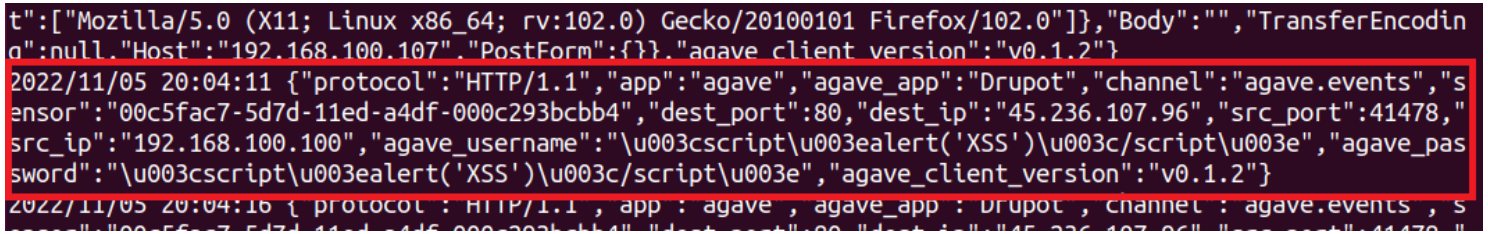
## Pruebas de funcionamiento del Honeypot Drupot

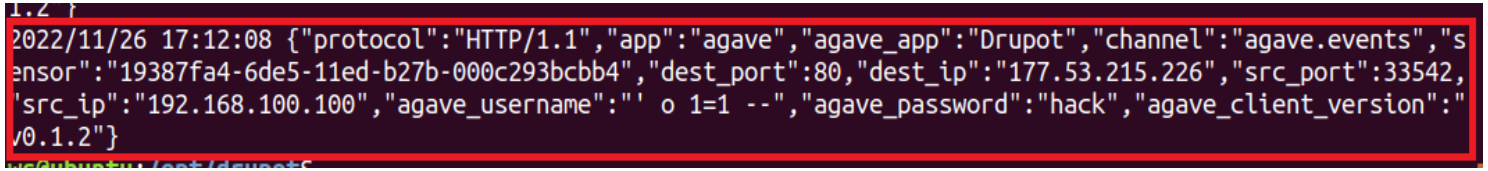
| | Name | Hostname | IP | Honeypot | UUID | Attacks |
|---|---|---|---|---|---|---|
| 1- | IoTWserver-agave | IoTWserver | 192.168.100.107 | agave | 81229a8c-5c80-11ed-9153-000c29b59cc7 | 4789 |



# RESULTADOS

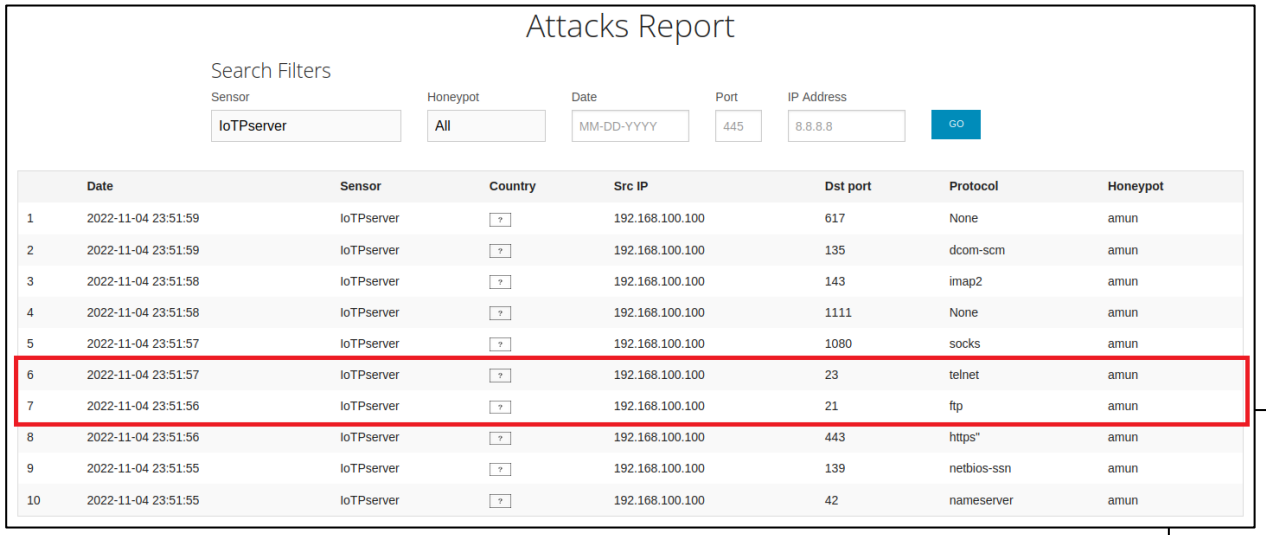
## Pruebas de funcionamiento del Honeypot Drupot



# RESULTADOS

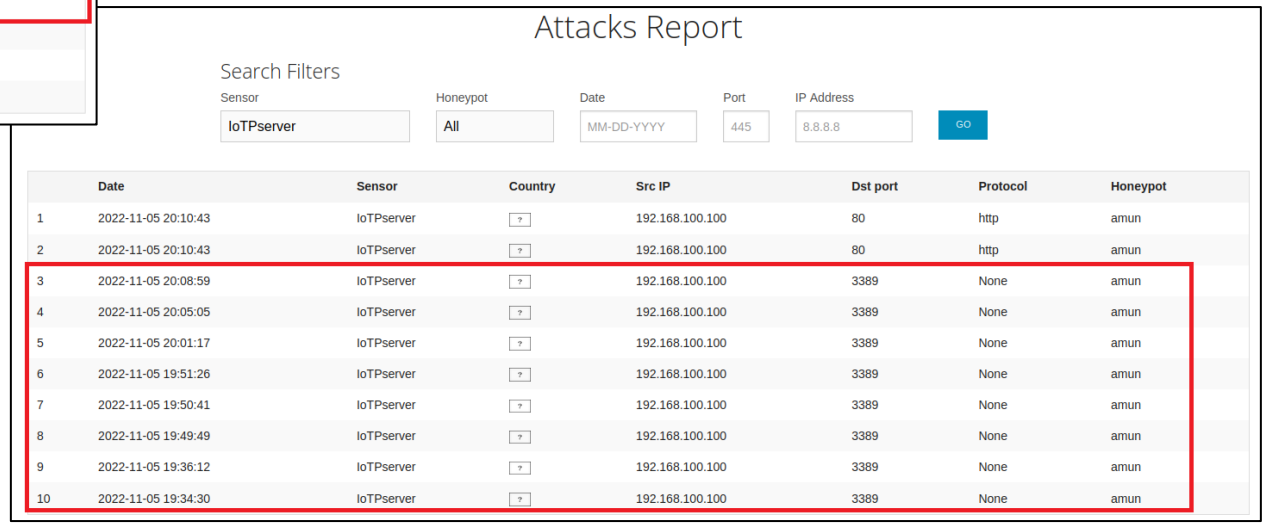
## Pruebas de funcionamiento del Honeypot Amun




| | Date | Sensor | Country | Src IP | Dst port | Protocol | Honeypot |
|---|---|---|---|---|---|---|---|
| 1 | 2022-11-04 23:51:59 | IoTPserver | ? | 192.168.100.100 | 617 | None | amun |
| 2 | 2022-11-04 23:51:59 | IoTPserver | ? | 192.168.100.100 | 135 | dcom-scm | amun |
| 3 | 2022-11-04 23:51:58 | IoTPserver | ? | 192.168.100.100 | 143 | imap2 | amun |
| 4 | 2022-11-04 23:51:58 | IoTPserver | ? | 192.168.100.100 | 1111 | None | amun |
| 5 | 2022-11-04 23:51:57 | IoTPserver | ? | 192.168.100.100 | 1080 | socks | amun |
| 6 | 2022-11-04 23:51:57 | IoTPserver | ? | 192.168.100.100 | 23 | telnet | amun |
| 7 | 2022-11-04 23:51:56 | IoTPserver | ? | 192.168.100.100 | 21 | ftp | amun |
| 8 | 2022-11-04 23:51:56 | IoTPserver | ? | 192.168.100.100 | 443 | https" | amun |
| 9 | 2022-11-04 23:51:55 | IoTPserver | ? | 192.168.100.100 | 139 | netbios-ssn | amun |
| 10 | 2022-11-04 23:51:55 | IoTPserver | ? | 192.168.100.100 | 42 | nameserver | amun |

```
2022-11-04 16:53:41,880 INFO [amun_request_handler] PortScan Detected on Port: 5000 (192.168.100.100)
2022-11-04 16:53:46,886 INFO [amun_request_handler] PortScan Detected on Port: 5000 (192.168.100.100)
2022-11-04 16:53:51,888 INFO [amun_request_handler] PortScan Detected on Port: 5000 (192.168.100.100)
2022-11-04 16:53:56,893 INFO [amun_request_handler] PortScan Detected on Port: 5000 (192.168.100.100)
2022-11-04 16:54:01,896 INFO [amun_request_handler] PortScan Detected on Port: 5000 (192.168.100.100)
2022-11-04 16:54:06,901 INFO [amun_request_handler] PortScan Detected on Port: 5000 (192.168.100.100)
2022-11-04 16:54:11,905 INFO [amun_request_handler] PortScan Detected on Port: 5000 (192.168.100.100)
2022-11-04 16:54:24,415 INFO [amun_request_handler] PortScan Detected on Port: 5000 (192.168.100.100)
2022-11-04 16:54:29,418 INFO [amun_request_handler] PortScan Detected on Port: 5000 (192.168.100.100)
```

```
2022-11-04 16:55:11,480 INFO [amun_request_handler] unknown vuln (Attacker: 192.168.100.100 Port: 8080) Mess
: ['POST /sdk HTTP/1.1\r\nConnection: close\r\nHost: 192.168.100.108:8080\r\nContent-Length: 441\r\nUser-Age
nt: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)\r\n\r\n<soap:Envelope xm
lns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:soap=
"http://schemas.xmlsoap.org/soap/envelope/"><soap:Header><operationID>00000001-00000001</operationID></soap:
Header><soap:Body><RetrieveServiceContent xmlns="urn:internalvim25"><_this xsi:type="ManagedObjectReference"
 type="ServiceInstance">ServiceInstance</_this></RetrieveServiceContent></soap:Body></soap:Envelope>'] (624)
 Stages: ['TIVOLI_STAGE1'])
```




| | Date | Sensor | Country | Src IP | Dst port | Protocol | Honeypot |
|---|---|---|---|---|---|---|---|
| 1 | 2022-11-05 20:10:43 | IoTPserver | ? | 192.168.100.100 | 80 | http | amun |
| 2 | 2022-11-05 20:10:43 | IoTPserver | ? | 192.168.100.100 | 80 | http | amun |
| 3 | 2022-11-05 20:08:59 | IoTPserver | ? | 192.168.100.100 | 3389 | None | amun |
| 4 | 2022-11-05 20:05:05 | IoTPserver | ? | 192.168.100.100 | 3389 | None | amun |
| 5 | 2022-11-05 20:01:17 | IoTPserver | ? | 192.168.100.100 | 3389 | None | amun |
| 6 | 2022-11-05 19:51:26 | IoTPserver | ? | 192.168.100.100 | 3389 | None | amun |
| 7 | 2022-11-05 19:50:41 | IoTPserver | ? | 192.168.100.100 | 3389 | None | amun |
| 8 | 2022-11-05 19:49:49 | IoTPserver | ? | 192.168.100.100 | 3389 | None | amun |
| 9 | 2022-11-05 19:36:12 | IoTPserver | ? | 192.168.100.100 | 3389 | None | amun |
| 10 | 2022-11-05 19:34:30 | IoTPserver | ? | 192.168.100.100 | 3389 | None | amun |



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# CONCLUSIONES

- El diseño de la solución de seguridad informática propuesta en el presente trabajo busca ser aplicable para la mayor cantidad de entornos basados en tecnologías de la información y comunicación. Si bien la arquitectura implementada se basa en un entorno del Internet de las Cosas, los honeypots pueden ser reemplazados en la fase de diseño para cubrir otras aristas y vectores de ataques dependiendo el ecosistema que se pretenda proteger. Así, se obtiene una arquitectura útil y configurable, lo que representa una ventaja hoy en día con el crecimiento tan acelerado de nuevas técnicas de intrusión y los procesos automatizados de ejecución de ataques.

- La honeynet híbrida propuesta permite repartir los señuelos en diferentes servidores creando redundancia en la arquitectura física de la solución. Se diseñó así con la finalidad de mantener totalmente operativa la red de señuelos. Al segregar los señuelos en diferentes servidores, se puede garantizar la operabilidad de la solución pese a alguna razón de mala configuración o ataque contra la integridad física de uno de estos sistemas. La honeynet híbrida seguirá recolectando y monitoreando los eventos de los honeypots que sigan funcionando correctamente.

# CONCLUSIONES

- El enfoque que se pretende cubrir con la implementación realizada es la detección de ataques automatizados y dirigidos a redes IoT que por su naturaleza se vuelven atractivas para atacantes, bots y amenazas desconocidas en la actualidad. Al utilizar honeypots de baja interacción se obtiene un sistema que atrae principalmente a bots configurados para detectar vulnerabilidades sobre entornos informáticos. Cabe indicar que el diseño no pretende generar una alta interacción con el atacante, si la finalidad fuese esta se seleccionará otro tipo de honeypots como los de interacción alta o inclusive de interacción media. Por este motivo esta solución de seguridad no será capaz de detectar ataques de día cero. Sin embargo, el diseño se puede acoplar para diferentes fines desde la protección de sistemas reales hasta entornos de investigación donde se pretenda recolectar técnicas más avanzadas utilizadas por ciberdelincuentes.

- El sistema fue sometido a pruebas de validación mediante una metodología de auditoría de seguridad informática. El fin de esta implementación fue garantizar la recolección de eventos perjudiciales que se generen a nivel de red. Consecuentemente las técnicas para validar el funcionamiento de estos señuelos son elementales. Como se mencionó anteriormente la arquitectura desplegada la componen principalmente señuelos de baja interacción como Dionaea, Amun aunque también se utiliza un honeypot que permite más interacción como Drupot. Estos señuelos son eficaces para detectar amenazas como bots que suelen ser programas informáticos que se encargan de la detección de vulnerabilidades de manera automática. Sin embargo, para ataques más sofisticados o ataques dirigidos esta elección de honeypots no es la más apropiada.

# CONCLUSIONES

- La configuración de la honeynet y la interconexión de los honeypots permitieron monitorear todos los eventos anómalos dentro de la red. Esta herramienta faculta al arquitecto de red la supervisión de dichos eventos y tomar mediadas proactivas mediante la caza de amenazas. La concentración de todos los registros en una base de datos facilitó el análisis de los logs generados. La interfaz web del servidor centralizado permitió obtener estadísticas en tiempo real de los eventos registrados y al estar todo catalogado se pudo identificar las direcciones IP de las principales amenazas.

- Se pudo apreciar que la solución implementada detecta ataques de escaneo de puertos, ataques sobre servicios específicos, inyecciones de código, ataques de denegación de servicio, entre otros. Adicionalmente, mediante el análisis de estos eventos se pudo determinar las técnicas utilizadas por la amenaza, como los scripts específicos utilizados para vulnerar cada honeypot, las peticiones empleadas y los hashes coincidentes de los exploits detectados. Esta herramienta cuenta con una biblioteca amplia de firmas que permiten reconocer y catalogar los ataques registrados. La solución implementada cubre las principales disposiciones y recomendaciones expuestas en normativas internacionales para la seguridad informática en el Internet de las Cosas.

# CONCLUSIONES

- La solución de seguridad es de fácil implementación y mantenimiento por lo que no requiere personal altamente calificado para la instalación de los señuelos y monitoreo de los eventos. Sin embargo, si se cuenta con un equipo de seguridad apropiado se puede interconectar este sistema con otras herramientas de correlación de eventos como un SIEM (Security Information and Event Management). Por consecuencia si la organización cuenta con un programa de seguridad se puede reforzar el esquema existente con el diseño propuesto. El servidor de registro MHN cuenta con un gran número de reglas implementadas, pero posibilita crear nuevas reglas a partir de los hallazgos de los eventos recolectados y las nuevas amenazas descubiertas.

- El hardware disponible para la implementación de la herramienta resultó ser apropiado y no limitó los requerimientos de operabilidad establecidos en su diseño. La Raspberry Pi es un excelente ordenador de placa reducida para la puesta en marcha de honeypots de baja interacción. Además de ser altamente portable y configurable reduce significativamente los costos de ejecución de la solución de seguridad. La limítate de utilizar señuelos de baja interacción es que en ataques realizados por un ciberdelincuente este puede reconocer que se trata de un sistema trampa.

# RECOMENDACIONES

- Antes de la implementación de la herramienta se debe realizar una evaluación de las necesidades de seguridad de la red donde se pretenda instalar la solución. Existen diversos tipos de honeypots que pueden ser adaptados y cada uno está diseñado para emular servicios específicos que probablemente sean de mayor utilidad en ciertas redes.

- El mantenimiento y la configuración del sistema de seguridad es sencillo sin embargo es aconsejable evaluar periódicamente el rendimiento de los dispositivos físicos que contienen la solución. Una política de mantenimiento de infraestructura.

- La gran cantidad de datos generados a causa de la recolección de logs provoca un uso alto de capacidad de memoria. En consecuencia, es recomendable contar con una política de respaldos para determinar la utilidad de los datos y almacenar la información generada de manera eficiente.

# TRABAJOS FUTUROS

- Implementación de otras herramientas de seguridad que complementen la funcionalidad de la solución de seguridad. Se puede abordar seguridad en redes inalámbricas con el uso de honeypots WiFI o también conocidos como hotspot para distraer y monitorear accesos no autorizados en redes WiFi.

- Despliegue de la solución de seguridad en otros sistemas de última generación. Se puede adaptar el diseño para entornos basados en la nube, Smart Cities, sistemas robóticos industriales y entornos domóticos basados en IoT. Esto permitirá obtener un espectro más amplio del panorama de amenazas que afecta a cada uno de estos ecosistemas.

- Creación de una herramienta mediante aprendizaje automático que permita captar e interpretar los datos recolectados por la Honeynet para ejecutar acciones de protección de manera autónoma sobre la red.