HONEYPOTS 101

Introducción a los HONEYPOTS

Presentación

- Miguel Raúl Bautista Soria
  - Miguel Bautista
    - Mike

- Security Researcher en Cisco TALOS (antes VRT)
  - Análisis e investigación de vulnerabilidades
  - Desarrollo de contenido de detección para Snort y ClamAV
- Anteriormente, 3 años en el UNAM-CERT en RIDI
- Chief Workshop Officer y Full member de The Honeynet Project

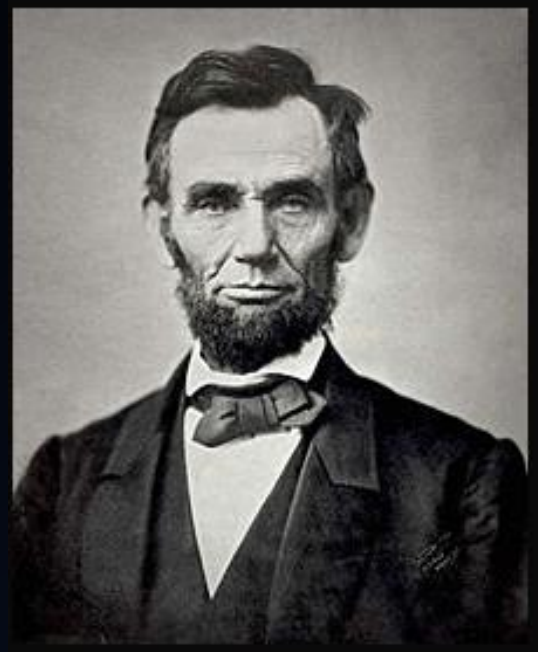
Temario

- Introducción e historia de los Honeypots
- Clasificación de los Honeypots
- Otros tipos de Honeypots
- Honeypots en la actualidad
- Implementación de Honeypots
- Analizando la información recolectada por un Honeypot
- Creación de un Honeypot

OBJETIVO

- Comprender qué es un Honeypot y cómo se usa.
- Revisar los distintos tipos de Honeypots.
- Conocer las herramientas existentes y cómo utilizarlas.
- Aprender los requisitos básicos para crear un Honeypot.

Introducción e historia

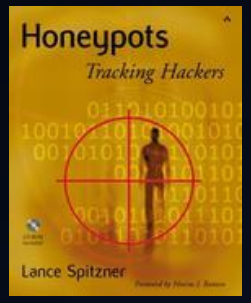


Una gota de miel caza más moscas que un galón de hiel.

(Abraham Lincoln)

¿Qué es un Honeypot?

- *Es un recurso de seguridad cuyo valor reside en ser identificado, atacado o comprometido*[1].



[1] Honeypots: Tracking Hackers. Lance Spitzner, Septiembre 2002.

¿Qué es un Honeypot? (En otras palabras)

- Es un equipo señuelo instalado en un punto de la red para poder recibir y, por lo tanto, detectar, tráfico malicioso o patrones relacionados.

¿Cuando surgen los Honeypots?

- 1986 – Clifford Stoll descubre una intrusión en una de las computadoras que administraba en el Laboratorio Nacional Lawrence Berkeley.
  - Libro: *The Cuckoo´s Egg.* Publicado en 1989 por el mismo Clifford Stoll.

ATTENTION: Mrs. Barbara Sherwin Document Secretary

SUBJECT: SDI Network Project

Dear Mrs. Sherwin:

I am interested in the following documents. Please send me a price list and an update on the SDI Network Project. Thank you for your cooperation.

Very truly yours,
Laszlo J. Balogh

#37.6 SDI Network Overview Description Document, 19 pages, December 1986

#41.7 SDI Network Functional Requirement Document, 227 pages, Revised September 1985

#45.2 Strategic Defense Initiations and Computer Network Plans and Implementations of Conference Notes, 300 Pages, June 1986

#47.3 SDI Network Connectivity Requirements, 65 pages, Revised April 1986

#48.8 How to Link to SDI Network, 25 pages, July 1986

#49.1 X.25 and X.75 Connection to SDI Network (includes Japanese, European, Hawaiian, 8 pages, December 1986)

#55.2 SDI Network Management Plan for 1986 to 1988, 47 pages, November 1986)

#62.7 Membership list (includes major connections), 24 pages, November 1986)

#65.3 List, 9 Pages, November 1986

"Hey Mike, remember those carrots I left out for bait in January?"
"You mean those SDI* files you concocted?"
"Yeah," I said. "Well, my dear, sweet, **nonexistent secretary** just received a letter."

*SDI: Strategic Defense Initiative

¿Cuando surgen los Honeypots?

- 1986 – Clifford Stoll descubre una intrusión en una de las computadoras que administraba en el Laboratorio Nacional Lawrence Berkeley.
  - Libro: *The Cuckoo´s Egg.* Publicado en 1989 por el mismo Clifford Stoll.
- 1991 – Bill Cheswick descubre a un atacante queriendo extraer información privada a través de un supuesto fallo de seguridad en un servidor de correo de los laboratorios Bell de AT&T.
  - Artículo: *An Evening with Berferd.* http://www.cheswick.com/ches/papers/berferd.pdf.

An Evening with Berferd
In Which a Cracker is Lured, Endured, and Studied

Bill Cheswick

AT&T Bell Laboratories

Abstract

On 7 January 1991 a cracker, believing he had discovered the famous sendmail DEBUG hole in our Internet gateway machine, attempted to obtain a copy of our password file. I sent him one.

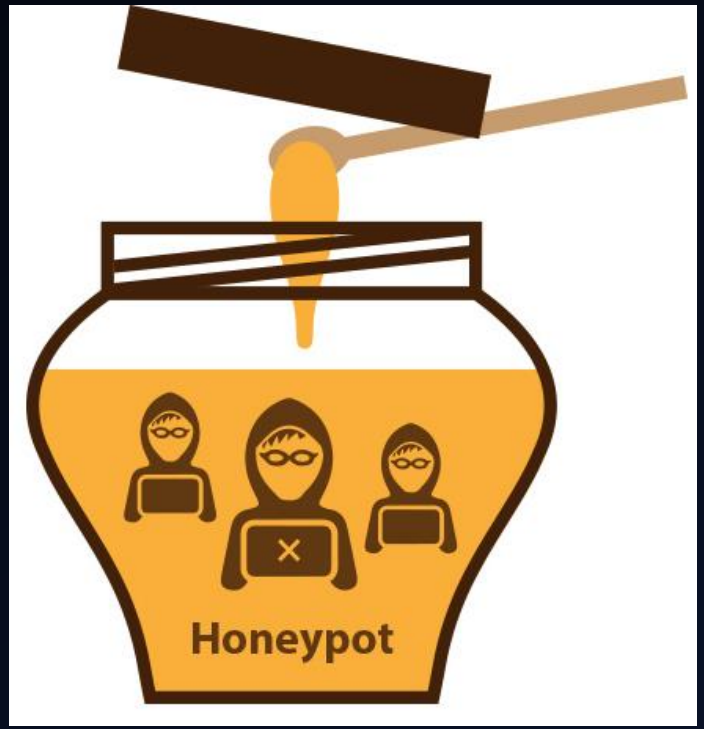
For several months we led this cracker on a merry chase in order to trace his location and learn his techniques. This paper is a chronicle of the cracker's "successes" and disappointments, the bait and traps used to lure and detect him, and the chroot "Jail" we built to watch his activities.

We concluded that our cracker had a lot of time and persistence, and a good list of security holes to use once he obtained a login on a machine. With these holes he could often subvert the *uucp* and *bin* accounts in short order, and then *root*. Our cracker was interested in military targets and new machines to help launder his connections.

¿Cuando surgen los Honeypots?

- 1999 – Surge The Honeynet Project, una organización sin fines de lucro establecida en Estados Unidos fundada por Lance Spitzner.
  - El objetivo principal de la organización es la investigación en el campo de los honeypots y las amenazas a la seguridad de la información.
  - Lance también introdujo por primera vez el término *honeynet*, el cual define como una red de honeypots de alta interacción que simulan una red en producción, configurada de manera que la actividad sea monitoreada, registrada y discretamente regulada.
  - https://www.honeynet.org/about

Clasificación de los honeypots



Clasificación de los honeypots

- Por su modo de funcionamiento:
  - Honeypots de baja interacción
  - Honeypots de alta interacción

- Por su entorno se dividen en:
  - Honeypots de producción
  - Honeypots de investigación

Honeypots de baja interacción

- Son equipos cuya característica principal es emular los servicios de un sistema real, con la finalidad de interactuar lo suficiente con los intrusos o amenazas automatizadas y recopilar datos.

- Son muy eficientes para la detección de patrones maliciosos, captura de malware y generación de estadísticas de tráfico en general.

- Fáciles de detectar.

Honeypots de alta interacción

- Son equipos reales y la interacción se da directamente con el software instalado en el sistema.

- Permite que los intrusos tengan un control mayor del sistema señuelo lo cual implica un mayor riesgo y, por lo tanto, la necesidad de un sistema de control externo que permita monitorear, almacenar y procesar la información capturada.

- Enfocado a un ámbito de investigación de las técnicas y tendencias de ataques de seguridad.

Honeypots de producción

- Son equipos situados en el entorno real de la red junto con otros equipos en producción como servidores.

- Comúnmente, son de baja interacción y funcionan como un complemento a la detección de amenazas, lo que mitiga de alguna manera los riesgos en la actividad de la red.

Honeypots de investigación

- Son equipos instalados con el único propósito de estudiar el comportamiento y las tendencias del tráfico malicioso causado por intrusos o ataques automatizados, situados en entornos exclusivos de prueba y, generalmente, con fines académicos.

- Tienen la característica de capturar y analizar la información, por lo que su configuración y administración puede ser más compleja.

Clasificación de los honeypots

- Por su modo de funcionamiento:
  - Honeypots de baja interacción.
  - Honeypots de alta interacción.

- Por su entorno se dividen en:
  - Honeypots de producción (baja interacción).
  - Honeypots de investigación (alta interacción).

comparativa

	Baja Interacción	Alta Interacción
Instalación	Fácil	Muy difícil
Mantenimiento	Fácil	Implica mucho tiempo
Riesgo	Bajo	Alto
Requiere control	No	Sí
Información recolectada	Reducida	Demasiada
Interacción	Servicios emulados	Control total

Ventajas de los honeypots

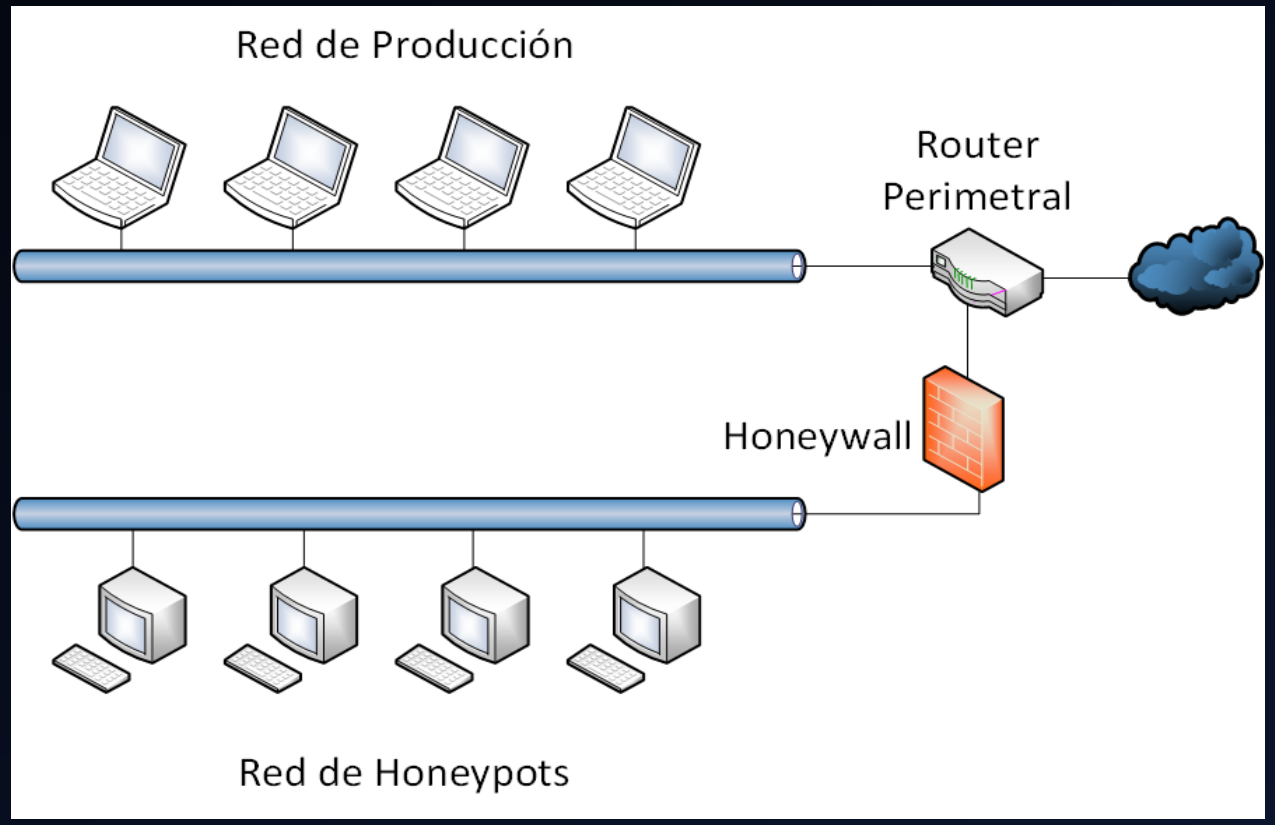
- Recolectan pequeños conjuntos de información.
- Reducen los falsos positivos.
- Pueden obtener falsos negativos.
- Trabajan en IPv6.
- Son muy flexibles.
- Requieren pocos recursos.
- Permiten descubrir nuevos ataques y tendencias.

desVentajas de los honeypots

- Tienen un alcance limitado.
- Riesgo de perder el control del equipo.
- Pueden ser identificados muy fácilmente.
- Eliminación o modificación de la evidencia, alterando el curso de la investigación.
- La actividad maliciosa identificada por los honeypots, no será representativa de la actividad presente en toda la red.
- Una muestra limitada de todas las amenazas en Internet.

honeynet

- Una Honeynet está formada por uno o más honeypots de alta interacción desplegados bajo un esquema de control y análisis de tráfico de red.

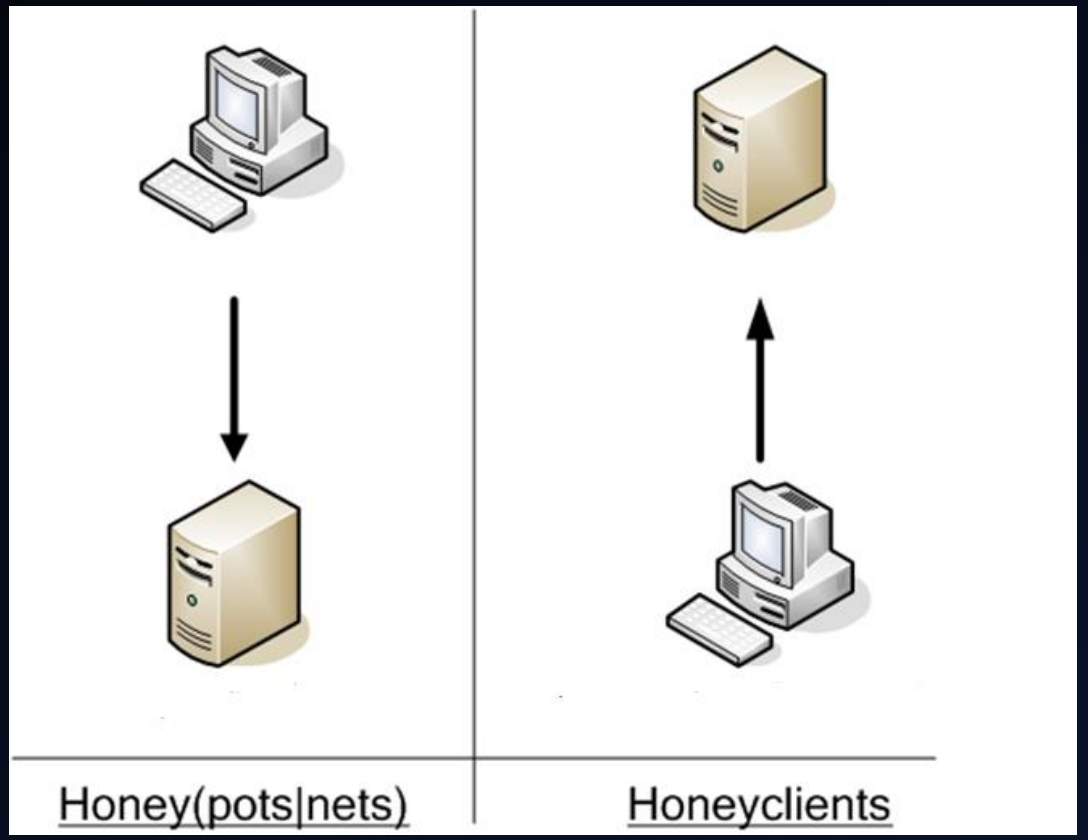


Otros tipos de honeypots: honeyclient

- Es una herramienta que permite identificar servidores maliciosos en Internet.
- Interactúa y analiza el contenido del servidor en busca de malware redirecciones, inyecciones de código, shellcodes, etc.
- Existen para los servicios más utilizados en Internet como SMTP, HTTP o FTP sin embargo, HTTP es en donde más efectividad se puede observar.

Otros tipos de honeypots: honeyclient

COMPARATIVA DE FUNCIONAMIENTO



Otros tipos de honeypots: honeyclient

OBJETIVOS:

- Evaluación / caracterización de sitios Web
- Pruebas de seguridad
- Detección de ataques 0 day
- Localizar vecinos problemáticos
- Obtención de malware y exploits

Otros tipos de honeypots: honeyclient

OBSOLETOS ANTE:

- Listas negras
- Cajas de diálogos
- Técnicas Anti-crawler
- Eventos dinámicos incrustados en páginas
- Comportamiento en la navegación

Honeypots en la actualidad

Glastopf

Cowrie

SSH/TELNET HONEYPOT

Honeypots en la actualidad

BAJA INTERACCIÓN

- Honeyd
- **Dionaea**
- Honeytrap
- **Glastopf**
- **Conpot**
- Kippo
- **Cowrie**
- **Snare**

ALTA INTERACCIÓN

- CaptureHPC (honeyclient)
- High Interacion Honeypot Analysis Toolkit
- SMB Honeypot
- Qebek
- Sebek

DIONAEA

- Es un honeypot de baja interacción
- Es una herramienta muy versátil para recolectar malware
- Actúa de manera pasiva emulando vulnerabilidades en servicios más comunes de Windows para recolectar información de ataques potenciales

glastopf

- Es un honeypot de baja interacción que emula un servidor web con varias páginas y aplicaciones con múltiples vulnerabilidades
- Permite detectar ataques de inyección SQL, XSS (Cross-Site-Scripting) y muchos más sobre páginas HTML
- Desarrollado por Lukas Rist del capítulo HoneyNor
- Enlace: https://github.com/mushorg/glastopf

conpot

- Es un honeypot de baja interacción para emular Sistemas de Control Industrial (SCADA) y obtener los métodos de ataque más comunes a estas plataformas
- Desarrollado por Lukas Rist y Johnny Vestergaard, ambos del capítulo HoneyNor
- Enlace: https://github.com/mushorg/conpot

kippo

- Es un honeypot de baja interacción que simula un servidor de Secure Shell (SSH) para detectar ataques de fuerza bruta en contraseñas, comandos más utilizados y registrar toda la actividad que genera un atacante al comprometer un servidor.

- Enlace: https://github.com/desaster/kippo

COWRIE

- Es un honeypot de baja interacción que también emula servidores SSH. Está basado en Kippo pero ahora contiene más soporte para comandos, acciones de los usuarios y nuevas características para hacerlo un servidor de Secure Shell indetectable.
- Desarrollado por Michel Oosterhof, miembro de Honeynet Project
- Enlace: http://www.micheloosterhof.com/cowrie/

ghost

- Es un honeypot para detectar y capturar malware que se auto propaga a través de memorias USB
- Funciona emulando un dispositivo USB en un equipo Windows
- Desarrollado por Sebastian Poeplau
- Enlace: https://github.com/honeynet/ghost-usb-honeypot

Implementación de honeypots

Implementación de honeypots

- La implementación dependerá completamente de lo que se quiera detectar:
  - Malware.
  - Vulnerabilidades nuevas o ya existentes.
  - Detección de ataques.
  - Análisis de la red.

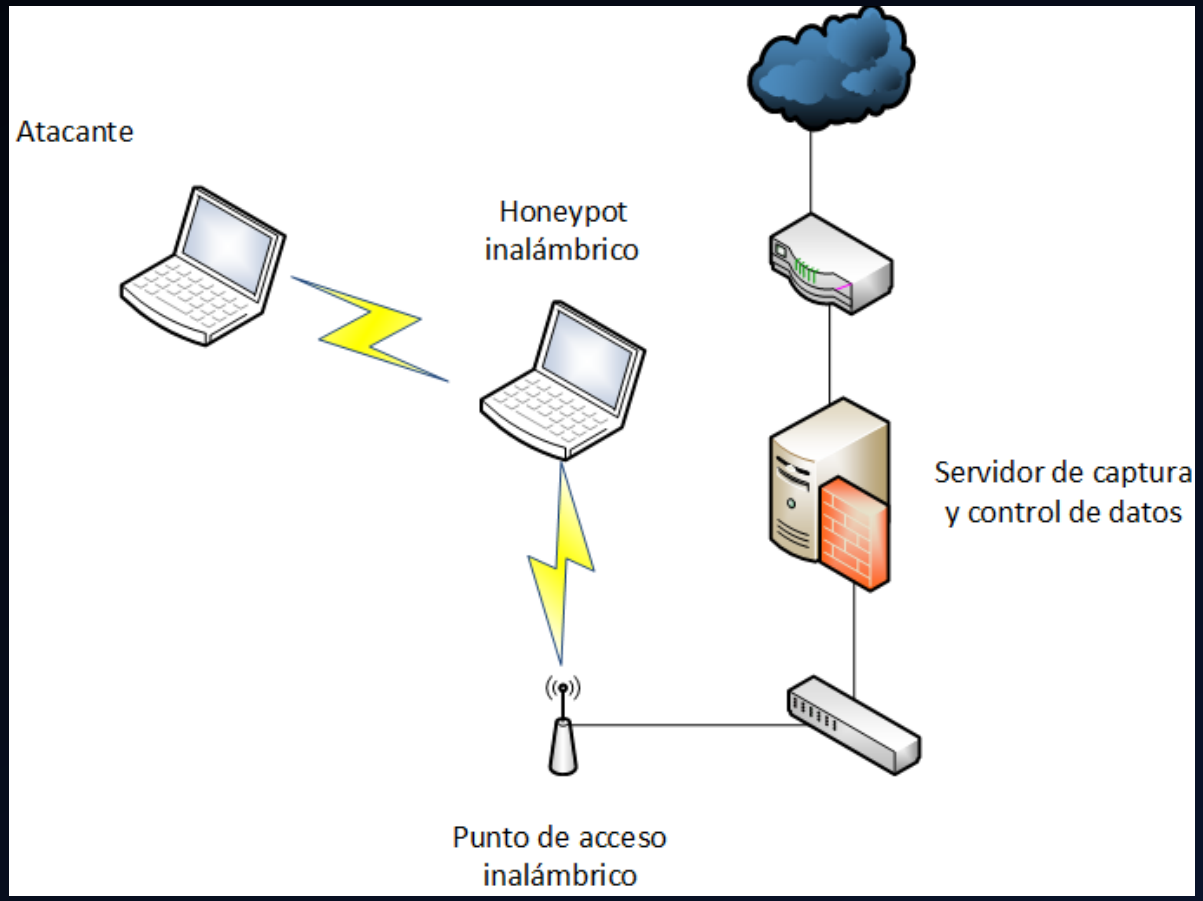
- También se debe contar con la infraestructura correcta y darle mantenimiento a los equipos en donde corran los Honeypots, la Honeynet, entre otras cosas.

- Se pueden utilizar otros recursos externos para mejorar nuestro ecosistema de seguridad.

Implementación de honeypots

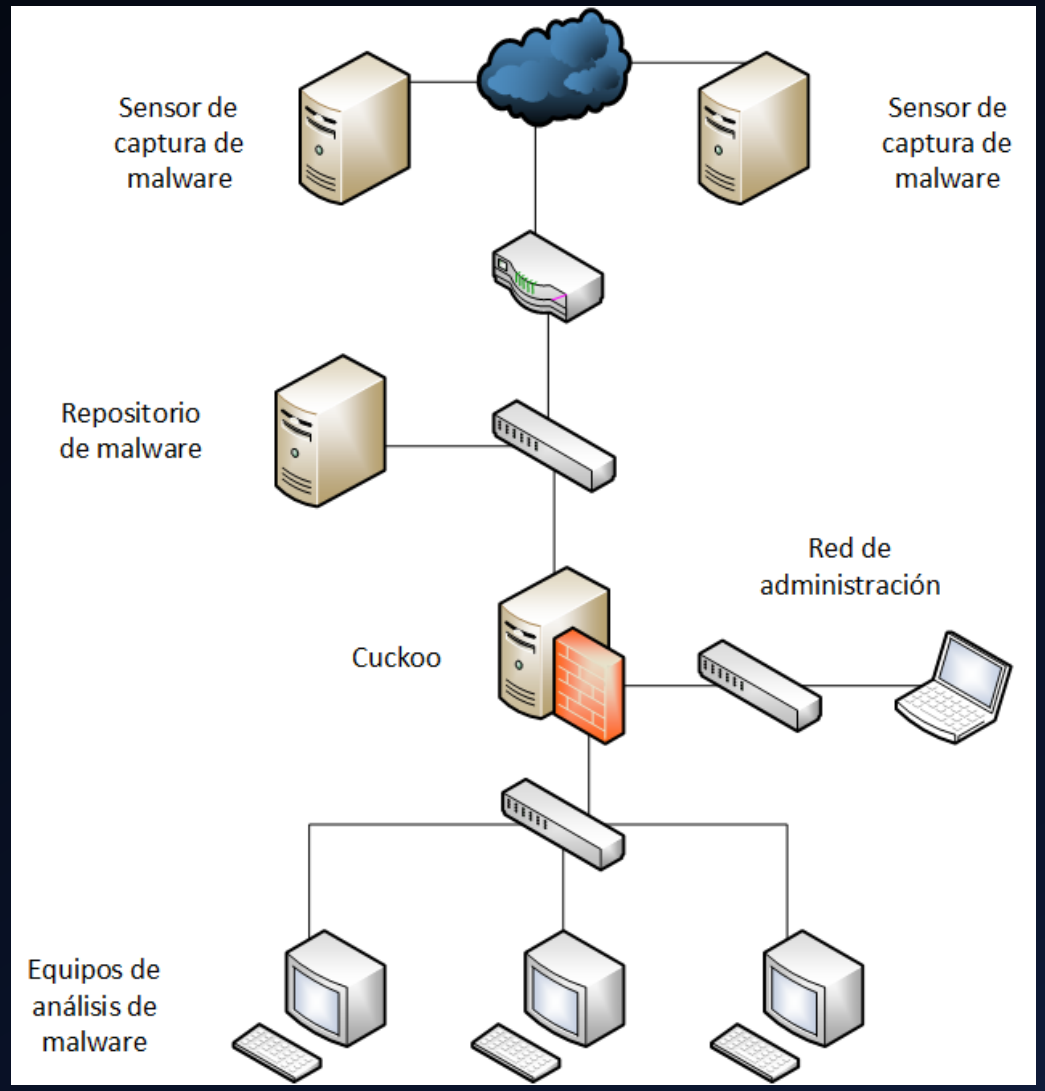
- Todos los Honeypots tienen su código libre y disponible para su descarga desde GitHub, sourceforge.net, google code, etc.
- Los Honeypots de baja interacción son los más fáciles de implementar.
- Se puede automatizar la generación de resultados de los Honeypots e incluso, procesar con scripts para obtener información digerible para el usuario.
- La utilización de Sandboxs públicas o privadas puede ayudar a disminiur significativamente la cantidad de amenazas nuevas o existents.
  - Cuckoo Sandbox
  - Hybrid Analysis
  - Joe Sandbox, etc.

Implementación de honeypots



Esbozo de laboratorio

- El malware se captura mediante honeypots
- Todo el tráfico de red es capturado:
  - Snort
  - Tcpdump
  - Cuckoo
- Todo el tráfico es controlado por:
  - IPS
  - Firewall
  - Cuckoo



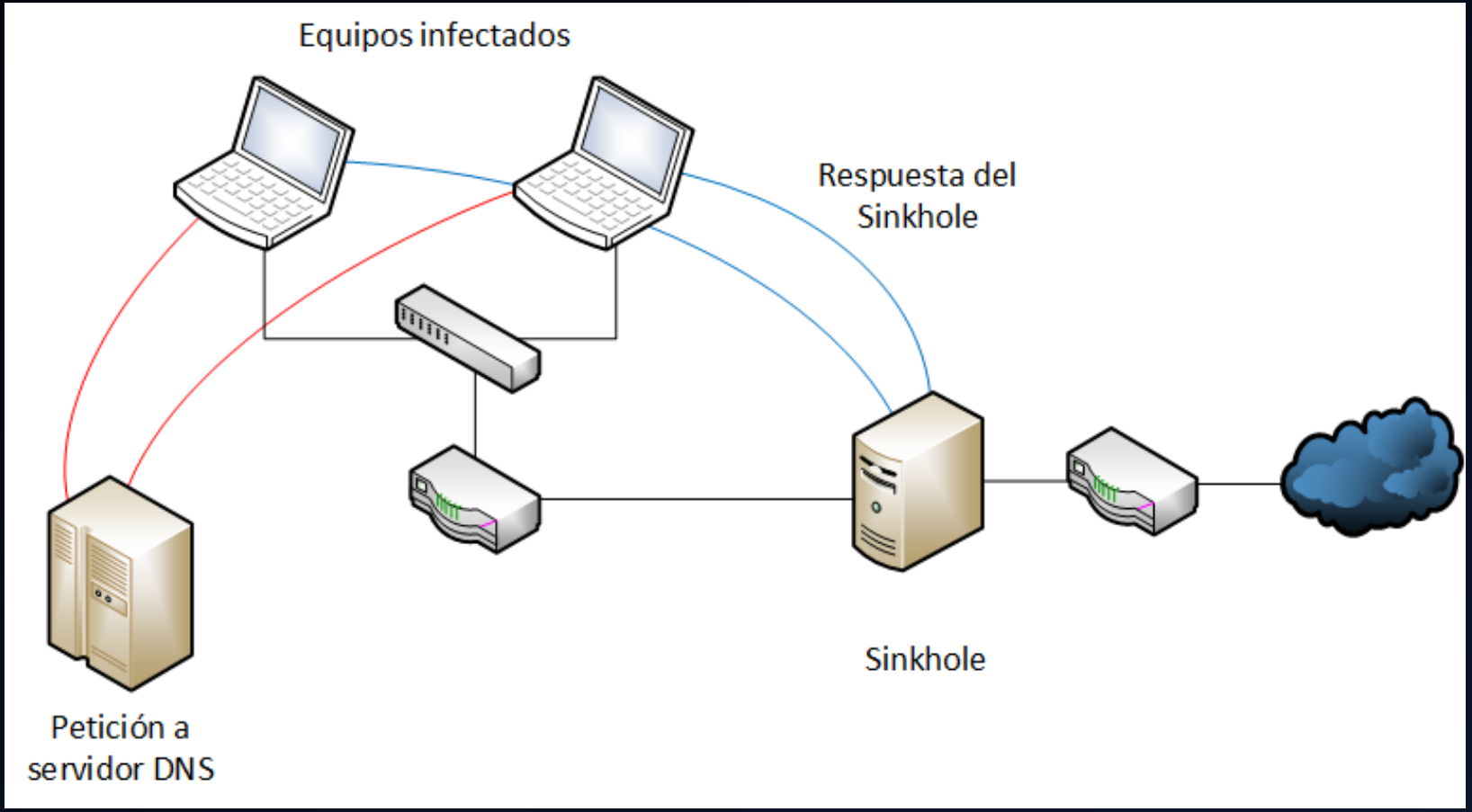
Uso de sinkhole

- Servidor que recibe, procesa y sirve peticiones maliciosas
- Permite realizar ingeniería inversa de malware, análisis de tráfico de red, etcétera
- Identificación de nombres de dominio maliciosos:
  - Botnets
  - Spyware
  - Phishing
  - Adware, etcétera

Uso de sinkhole

- Se requiere de la configuración de un servidor DNS para redirigir peticiones maliciosas al Sinkhole
- Recibirá las peticiones del protocolo HTTP e IRC
- Servirá un archivo ficticio en caso de que se haya recibido una solicitud por HTTP
- Servirá un servidor de chat IRC, así como los canales y comandos básicos para interactuar con el malware
- Registrará toda la actividad solicitada
- Como extra, recibirá tráfico diferente de HTTP e IRC que podría ser analizado con algún IDS local

Uso de sinkhole



Uso de darknets

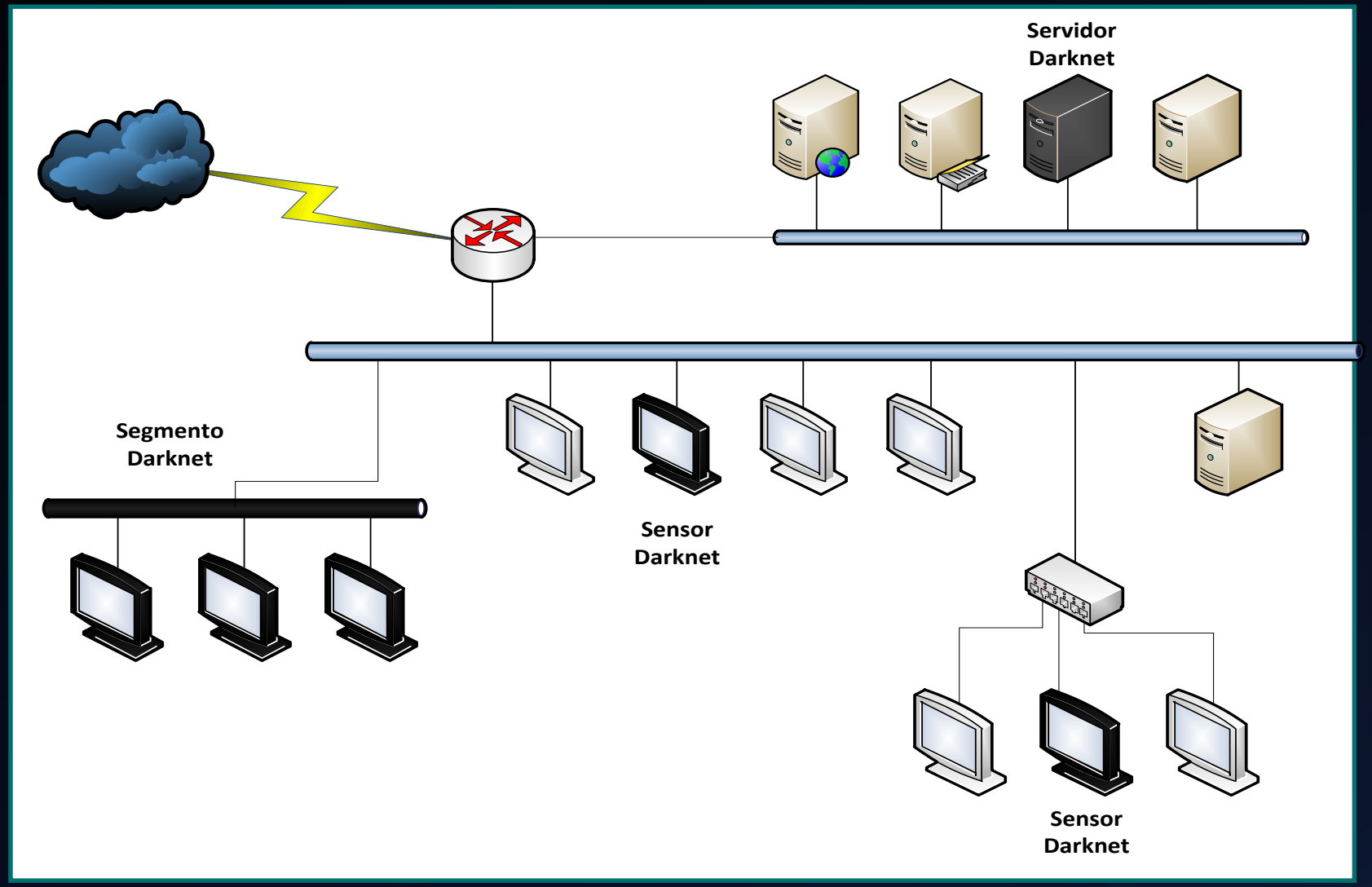
- Significado de una Darknet:

- Es un equipo o conjunto de ellos que utilizan direcciones IP o segmentos de red que no están asignados a ningún servicio o dispositivo específico dentro de un entorno de red.
- Todas las direcciones IP de la darknet están explícitamente reservadas para no ser asignadas a algún equipo de la red de producción.

Uso de darknets

- El tráfico no asignado corresponde al relacionado con todas las direcciones IP de la darknet.
- En un entorno ideal este tráfico no debería existir, sin embargo, es importante mencionar que el hecho de que exista no necesariamente significa que haya actividad maliciosa en la red, ya que puede deberse también a alguna anomalía en la configuración de algún equipo o dispositivo de enrutamiento.
- El número de direcciones IP destinadas a la darknet es proporcional a la cantidad de eventos detectados y dependiendo de las características y capacidades de implementación, es también proporcional a la efectividad de la información analizada.

Uso de darknets



Creación de un honeypot

- Creación de un Honeypot para correo SMTP
- Requisitos:
  - Saber programar.
  - Identificar el tipo de Honeypot que se requiera crear.
  - Una vez identificado el tipo de Honeypot deseado, se recomienda definir el alcance del Honeypot.
  - Leer la documentación correcta del servicio, RFC o herramienta, que le haya llamado la atención para empezar a programar las acciones del Honeypot.
  - Definir la forma de entrega de resultados, para que se ajuste a las necesidades del usuario final.
  - Manos a la obra!

REFERENCIAS

- https://github.com/paralax/awesome-honeypots
- https://hub.docker.com/u/honeynet/

Gracias!

MIGUEL ´MIKE´BAUTISTA

@MIGUELRAULB
MIGUELRAULB@GMAIL.COM