A picture containing text, clipart

Description automatically generatedA picture containing diagram

Description automatically generatedUniversidad Tecnológica de Panamá

Facultad de Ingeniería de Sistemas Computacionales

Licenciatura en Ingeniería en Sistemas de Información

Seguridad Informática

Parcial #2

Integrantes:

Cutire, Fernando 8-972-906

Díaz, Gabriel (20-53-5198)

Jonathan Gamero (8-982-2008)

Grupo 1IF131

Profesor: José Moreno

I Semestre

2022

# Índice de Contenidos

[Índice de Contenidos 2](#_Toc108120355)

[INTRODUCCCIÓN 3](#_Toc108120356)

[OBJETIVO: 3](#_Toc108120357)

[PERFIL DEL PROYECTO 3](#_Toc108120358)

[MARCO TEÓRICO 4](#_Toc108120359)

[¿Qué es un honeypot? 4](#_Toc108120360)

[¿Cómo funcionan los honeypots? 4](#_Toc108120361)

[Los peligros de los honeypots 4](#_Toc108120362)

[Procedimiento: Desarrollo del taller 5](#_Toc108120363)

[Paso 1: Disco Honeydrive 5](#_Toc108120364)

[Paso 2: Máquina Virtual 5](#_Toc108120365)

[Paso 3: Iniciando comando en Terminal 7](#_Toc108120366)

[Paso 4: ifconfig 7](#_Toc108120367)

[Paso 5. Accediendo al navegador 8](#_Toc108120368)

[Paso 6: Máquina virtual con Kali Linux 8](#_Toc108120369)

[Paso 7: Descarga del archivo rockyou.txt 9](#_Toc108120370)

[Paso 8: Empleando Medusa 9](#_Toc108120371)

[Paso 9 : Kippo-graph 10](#_Toc108120372)

[Análisis de resultados 12](#_Toc108120373)

[Top 10 de contraseñas usadas 12](#_Toc108120374)

[Top 10 de nombres de usuarios usados 12](#_Toc108120375)

[Top 10 de contraseñas y nombre de usuario usados para el intento de ataque 13](#_Toc108120376)

[Grafica de top 10 de contraseñas y nombre de usuario usados para el intento de ataque 13](#_Toc108120377)

[Ratio de ataques 14](#_Toc108120378)

[Grafica de IP usadas para realizar los intentos de ataques 14](#_Toc108120379)

[Pruebas por día 15](#_Toc108120380)

[Top 10 de los ssh clientes más usados 16](#_Toc108120381)

[Conclusiones 17](#_Toc108120382)

[Bibliografía y Referencias 18](#_Toc108120383)

# INTRODUCCCIÓN

El siguiente trabajo presentado es una implementación de una herramienta de seguridad para atraer atacantes desprevenidos y analizar los ataques que realicen a infraestructura critica.

Para ello utilizaremos una herramienta de honeypot que emule dicha infraestructura critica utilizando dos máquinas virtuales distintas, una que simule al atacante y la otra será nuestro honeypot con un mínimo de 3 servicios emulados.

## OBJETIVO:

Implementar honeypot herramienta de seguridad informática para atraer atacantes y analizar comportamientos de los ataques que realizan a infraestructuras críticas.

## PERFIL DEL PROYECTO

Deberán implementar una herramienta de honeypot que emule infraestructura de seguridad crítica y que permita recolectar estadística, vulnerabilidad, herramientas utilizadas, como mínimo con 3 servicios emulados.

# MARCO TEÓRICO

## ¿Qué es un honeypot?

En términos de seguridad informática, una trampa cibernética funciona de manera similar, provocando una trampa para los piratas informáticos. Es un sistema informático de sacrificio que pretende atraer ataques cibernéticos, como un señuelo. Imita un objetivo para los piratas informáticos y utiliza sus intentos de intrusión para obtener información sobre los ciberdelincuentes y la forma en que operan o para distraerlos de otros objetivos.

## ¿Cómo funcionan los honeypots?

El honeypot parece un sistema informático real, con aplicaciones y datos, lo que engaña a los ciberdelincuentes haciéndoles creer que es un objetivo legítimo. Por ejemplo, un honeypot podría imitar el sistema de facturación de clientes de una empresa, un objetivo frecuente de ataque para los delincuentes que desean encontrar números de tarjetas de crédito. Una vez que los piratas informáticos están dentro, se pueden rastrear y evaluar su comportamiento en busca de pistas sobre cómo hacer que la red real sea más segura.

## Los peligros de los honeypots

Si bien la ciberseguridad del honeypot ayudará a trazar el entorno de amenazas, los honeypots no verán todo lo que está sucediendo, solo la actividad dirigida al honeypot. Solo porque una determinada amenaza no se haya dirigido contra el honeypot, no puede asumir que no existe; es importante mantenerse al día con las noticias de seguridad de TI, no solo confiar en los honeypots para que le notifiquen las amenazas.

Una vez que se ha "tomado la huella digital" de un honeypot, un atacante puede crear ataques falsificados para distraer la atención de un exploit real dirigido contra sus sistemas de producción. También pueden enviar mala información al honeypot.

Peor aún, un atacante inteligente podría potencialmente usar un honeypot como una forma de ingresar a sus sistemas. Es por eso que los honeypots nunca pueden reemplazar los controles de seguridad adecuados, como los firewalls y otros sistemas de detección de intrusos. Dado que un honeypot podría servir como plataforma de lanzamiento para una mayor intrusión, asegúrese de que todos los honeypots estén bien asegurados. Un 'honeywall' puede proporcionar la seguridad básica del señuelo y evitar que los ataques dirigidos contra el señuelo entren en su sistema en vivo

# Procedimiento: Desarrollo del taller

## Paso 1: Disco Honeydrive

Primero importaremos la imagen de disco honeydrive

Graphical user interface, text, application, email

Description automatically generated

## Paso 2: Máquina Virtual

Iniciamos la máquina virtual, debe aparecernos algo como esto

Graphical user interface

Description automatically generated with low confidence

## Paso 3: Iniciando comando en Terminal

Luegoabriremos la terminal donde colocaremos el siguiente comando **/honeydrive/kippo/start.sh** para activar el Kippo que es la herramienta que usamos para detención de intruso. Y se conecta por medio de ssh .

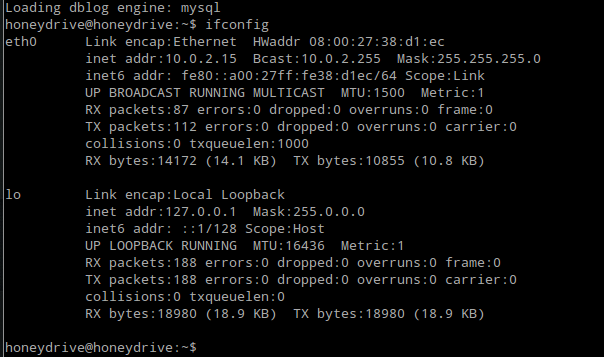
Lo que nos da como resultado lo siguiente:

Text

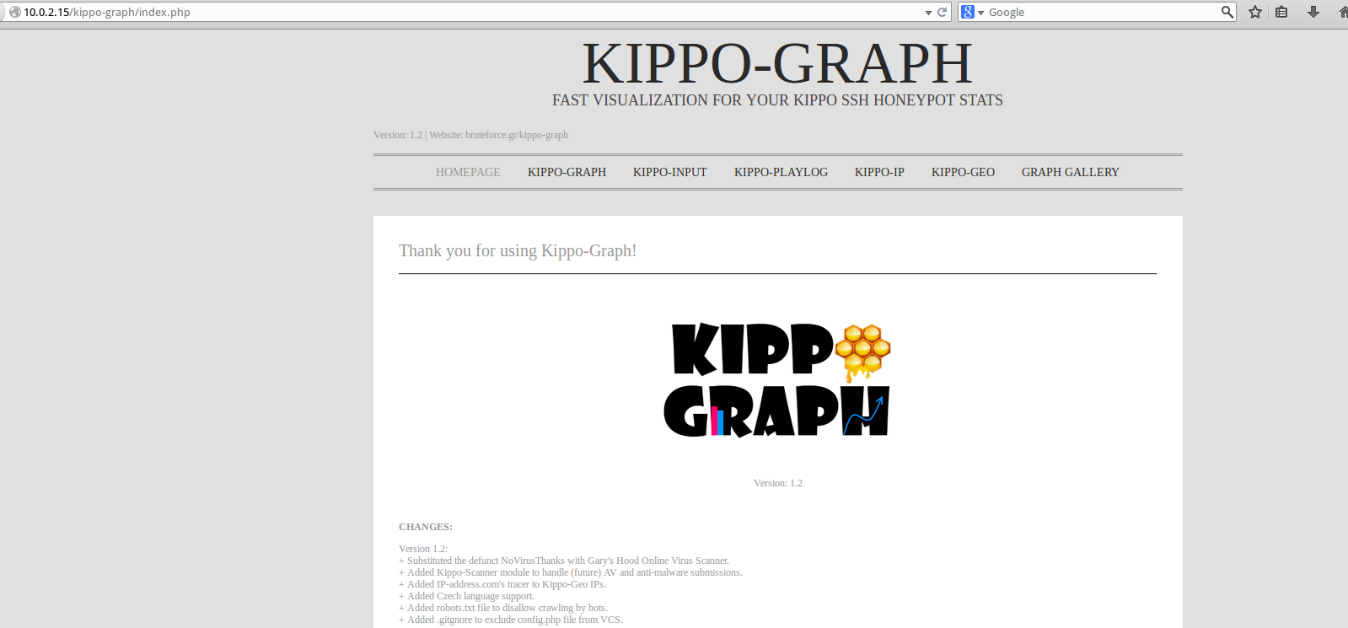
Description automatically generated

## Paso 4: ifconfig

Luego utilizaremos el comando **ifconfig** para buscar la ip



## Paso 5. Accediendo al navegador

Abriremos el navegador donde buscaremos http://10.0.2.15/kippo-graph/ para acceder a kippo-Graph

## Paso 6: Máquina virtual con Kali Linux

Luego en el VirtualBox abrimos Kali Linux y buscamos la terminal escaneamos la IP del honeydrive para comprobar que hay latencia pues se usara la maquina virtual de kali como equipo que atacara.se usa el código **nmap –sP 10.0.2.15**

Graphical user interface, text, chat or text message

Description automatically generated

Podemos observar que el host se encuentra activo

## Paso 7: Descarga del archivo rockyou.txt

Descargamos el archivo rockyou.txt utilizando el navegador

Graphical user interface, application

Description automatically generated

## Paso 8: Empleando Medusa

Utilizaremos el comando **medusa –h 192.168.56.109 –P /home/kali/Desktop/rockyou.txt –u honeydrive –n 22 –M ssh**

Text

Description automatically generated

## Paso 9 : Kippo-graph

Buscamos kippo-Graph y podremos visualizar lo siguiente:

Graphical user interface, text, application

Description automatically generated

Total, de intentos de login, cuantos IP fueron utilizadas, fechas en el que se hizo el primer intento de ataque y el ultimo.

A screenshot of a computer

Description automatically generated

# Análisis de resultados

## Top 10 de contraseñas usadas

Chart, bar chart, histogram

Description automatically generated

## Top 10 de nombres de usuarios usados

Chart

Description automatically generated

## Top 10 de contraseñas y nombre de usuario usados para el intento de ataque

Graphical user interface, application

Description automatically generated

Grafica de top 10 de contraseñas y nombre de usuario usados para el intento de ataque   
Chart, pie chart

Description automatically generated

## Ratio de ataques

Chart

Description automatically generated

## Grafica de IP usadas para realizar los intentos de ataques

Chart

Description automatically generated

Graphical user interface, bubble chart

Description automatically generated

Pruebas por díaGraphical user interface

Description automatically generated

## Top 10 de los ssh clientes más usados

Graphical user interface, application

Description automatically generated

# Conclusiones

* Los honeypots son una herramienta muy potente para el análisis y la defensa de sistemas informáticos, siempre y cuando presenten una configuración de seguridad correcta para evitar que sirvan de punto de entrada de amenazas y se tengan en cuenta todas sus ventajas e inconvenientes.
* Los Honeypot nos aportan la posibilidad de saber cómo nos están atacando, e intentar descubrir quién es el atacante. Es decir, los honeypot son una función de control adicional respecto a la seguridad, para saber cómo actuar en caso de recibir un ataque, ya que sabremos cómo actúan gracias al estudio previo del equipo de seguridad que se encargue de controlar estos Honeypot.
* La principal ventaja de estos sistemas Honeypot para los equipos de ciberseguridad son que pueden obtener datos muy relevantes de los ataques recibidos, y saber cómo solucionarlos o mitigarlos gracias al estudio previo.

# Bibliografía y Referencias

Descifrado de contraseñas con Medusa en Linux – Acervo Lima. (n.d.). Retrieved June 23, 2022, from Acervolima.com website: https://es.acervolima.com/descifrado-de-contrasenas-con-medusa-en-linux/

Burns, W. J. (2019). Common Password List ( rockyou.txt ) [Data set].