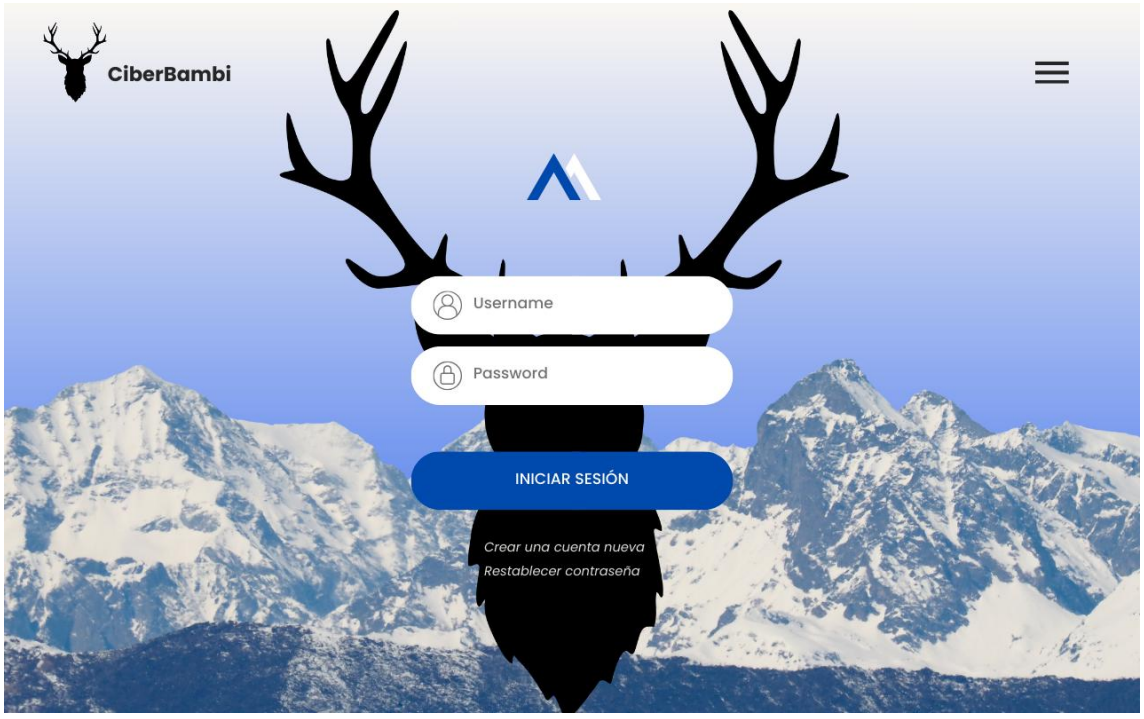
PROYECTO INTERMODULAR ASIX

Ciberbambi

Honeypots



Configurado por Adam Valien y documentado por Sergi Couto.

Miembros:

Adam Valien, Adam Ahmadi y Sergi Couto.

Contenido

1. ¿Qué es un Honeypot?

Un **honeypot** es un sistema o servicio diseñado para **simular ser vulnerable o atractivo para un atacante**, con el objetivo de:

- Detectar intentos de intrusión.
- Analizar el comportamiento de atacantes.
- Registrar evidencias de ataques reales.
- Mejorar la seguridad del sistema real.

A diferencia de un sistema productivo, un honeypot **no debería recibir tráfico legítimo**, por lo que **cualquier conexión es sospechosa**.

2. Tipos de Honeypots según el mercado

Actualmente existen distintos tipos de honeypots, que se pueden clasificar según su **nivel de interacción**, su **finalidad** y el **servicio que simulan**.

2.1 Según el nivel de interacción

Honeypots de baja interacción

- Simulan servicios básicos (SSH, HTTP, FTP...).
- No ofrecen un sistema real completo.
- Son fáciles de configurar y mantener.
- Bajo riesgo de compromiso.

Honeypots de media interacción

- Simulan servicios de forma más realista.
- Permiten cierta interacción con el atacante.
- Requieren más configuración y control.

Honeypots de alta interacción

- Sistemas reales completos y vulnerables.
- El atacante puede moverse libremente.
- Riesgo elevado si no están bien aislados.
- Uso más profesional o de investigación.

2.2 Según el servicio que simulan

Honeypots web → simulan páginas web vulnerables.
Honeypots de red → capturan tráfico malicioso.
Honeypots de servicios → SSH, FTP, SMTP, MySQL, etc.
Honeypots de malware → capturan muestras de virus.

3. Honeypot elegido para el proyecto: T-Pot

Para la realización de esta fase del proyecto se ha optado por utilizar **T-Pot**, una plataforma de honeypots desarrollada por Telekom Security.

3.1 ¿Qué es T-Pot?

T-Pot es una distribución Linux basada en Debian que integra múltiples honeypots de forma centralizada, junto con herramientas de monitorización, registro y visualización de ataques.
Su principal ventaja es que permite desplegar **varios honeypots al mismo tiempo**, simulando diferentes servicios vulnerables y facilitando la recogida de evidencias desde una única interfaz.

3.2 Motivos de la elección de T-Pot

Se ha elegido T-Pot por los siguientes motivos:

- Integra **varios honeypots de baja y media interacción**.
- Incluye herramientas de **visualización de logs** (Kibana).
- Es ampliamente usado en entornos educativos y de investigación.
- Permite obtener **evidencias claras y reales** de ataques.
- Se ajusta al nivel formativo de **Administración de Sistemas**.
- Reduce la complejidad de instalar honeypots por separado.

3.3 Honeypots incluidos en T-Pot

T-Pot incluye distintos honeypots que simulan servicios reales atacados habitualmente:
Cowrie → SSH y Telnet
Dionaea → Malware y exploits
Honeytrap → Puertos genéricos
ElasticPot → Elasticsearch
ConPot → Sistemas industriales (ICS)
Suricata → Detección de intrusiones (IDS)

4. Arquitectura y entorno de despliegue

4.1 Entorno utilizado

T-Pot se ha desplegado en una **máquina virtual**, con el objetivo de garantizar el aislamiento y la seguridad del entorno.

Características generales:

- Sistema operativo: Debian (imagen oficial T-Pot)
- Tipo: Máquina virtual
- Acceso: Red controlada
- Uso exclusivo como honeypot

4.2 Medidas de seguridad

Para minimizar riesgos:

- La máquina está **aislada del entorno productivo**.
- No contiene información sensible.
- No tiene acceso a la red interna.
- Solo se permite el tráfico necesario para el funcionamiento del honeypot.

5. Instalación y configuración de T-Pot

5.1 Descarga e instalación

La instalación se realiza mediante la **imagen oficial ISO de T-Pot**, siguiendo el asistente de instalación.

Pasos generales:

- Descarga de la imagen oficial.
- Creación de máquina virtual.
- Asignación de recursos (CPU, RAM y disco).
- Instalación guiada del sistema.
- Configuración inicial de red y credenciales.

5.2 Acceso a la plataforma

Una vez instalado, T-Pot proporciona:

- Acceso web a la consola de visualización.
- Acceso SSH para administración.
- Panel de control con estadísticas de ataques.

6. Evidencias y registros obtenidos

Uno de los principales objetivos del uso de T-Pot es la **obtención de evidencias reales de ataques**.

6.1 Tipos de registros recogidos

T-Pot registra automáticamente:

- Direcciones IP atacantes.
- Puertos más atacados.
- Servicios objetivo.
- Intentos de autenticación.
- Comandos ejecutados por atacantes.
- Fecha y hora de los ataques.

6.2 Visualización de ataques

Los datos recogidos se visualizan mediante:

- **Kibana**, para gráficos y estadísticas.
- Logs del sistema.
- Registros individuales de cada honeypot.

Ejemplos de evidencias:

- Intentos de fuerza bruta por SSH.
- Escaneos de puertos automáticos.
- Descarga de malware.
- Ataques repetidos desde la misma IP.

7. Análisis de los resultados

Tras un periodo de funcionamiento, se ha observado que:

- Los servicios más atacados son **SSH y puertos comunes**.
- Muchos ataques son **automatizados** mediante bots.
- Se repiten usuarios y contraseñas comunes.
- Existen escaneos constantes incluso sin publicidad del sistema.

Esto demuestra que un sistema expuesto a Internet **recibe ataques de forma continua**, aunque no contenga información relevante.

8. Conclusión

La implementación de **T-Pot como honeypot** ha permitido:

- Analizar ataques reales en tiempo real.
- Centralizar la gestión de múltiples honeypots.
- Obtener evidencias claras y documentables.
- Comprender mejor las técnicas utilizadas por atacantes.
- Reforzar la importancia de la seguridad en sistemas expuestos.

T-Pot se presenta como una **herramienta muy completa y adecuada para entornos educativos**, especialmente en ciclos formativos de **Administración de Sistemas**.