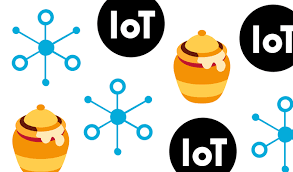
**Analizando al enemigo Honeypot**



Daniel Escaño Hernández CET Ciberseguridad

# 

# 

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **2**

[**2. Descargamos la ISO**](#_ilx67fbw82ie) **3**

[**3. Creación e instalación de la maquina**](#_p29m2jupa7e1) **3**

[**4. Acceso, actualización**](#_ikem0xby4bx4) **4**

[**5. Configuración**](#_k6o27oyycr0e) **5**

[**6. Configuración Red**](#_mtdld2h8jyz1) **6**

[**7. Configuración y Acceso Web**](#_li2hpcdljz7a) **7**

[**8. Escaneo de puertos y conexión SSH**](#_dqsydgooanv0) **8**

[**9. Ataque SSH**](#_lpcesa1ar53b) **9**

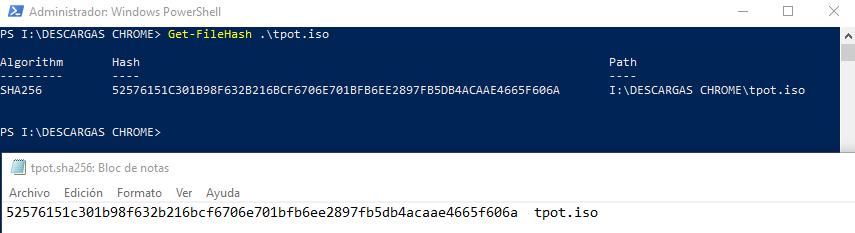
# 

# **2. Descargamos la ISO**

Descargamos la ISO de T-Pot del siguiente repositorio:

https://github.com/telekom-security/tpotce/releases

Comprobar la descarga mediante el archivo resumen SHA256.

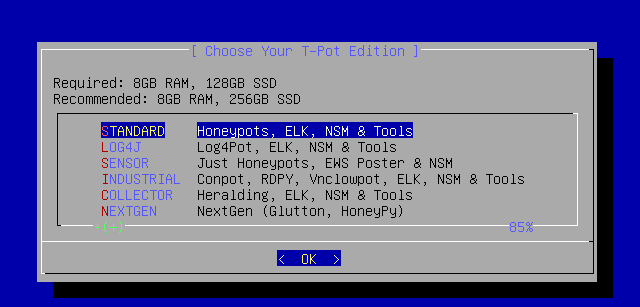


# **3. Creación e instalación de la maquina**

Crear una máquina virtual con 6GB RAM y 15 GB de disco duro.

(a) Instalar el T-Pot (seleccionar mirror de archivo Debian en la instalación). Antes de esta parte nos pedirá seleccionar el idioma, zona horaria,…

(b) Seleccionar la opción STANDARD. Primero nos pedirá la contraseña de acceso por consola (dos veces). Luego establecer nombre de usuario contraseña y nombre de usuario para el acceso vía web (dos veces). El usuario por defecto es tsec (no se podrá usar para el acceso web)



# 

# 

# **4. Acceso, actualización**

Acceder con el usuario configurado y ponernos como root para actualizar la máquina.

Utilizaremos los siguientes comandos:

sudo su

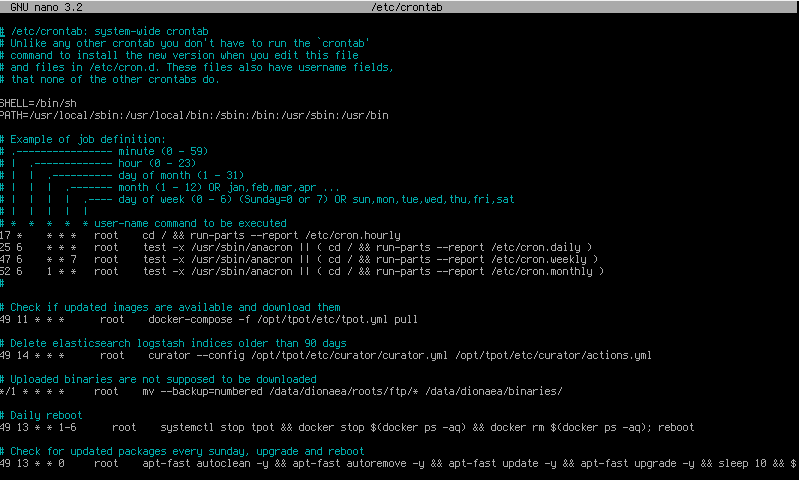
cd opt/tpot

sudo ./update.sh -y



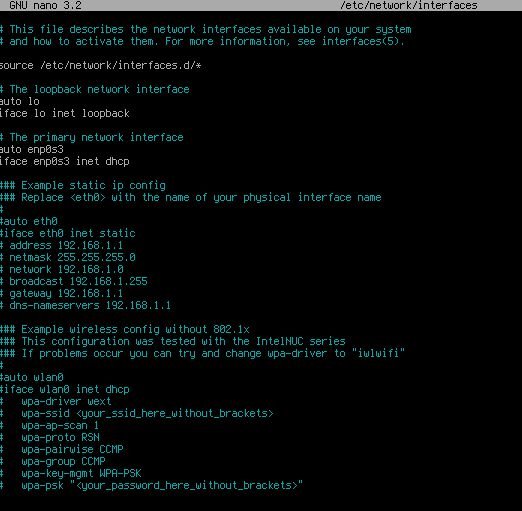
# **5. Configuración**

T-Pot se reinicia diariamente para comprobar la integridad de los contenedores, podemos editarlo en /etc/crontab (tarea programada)



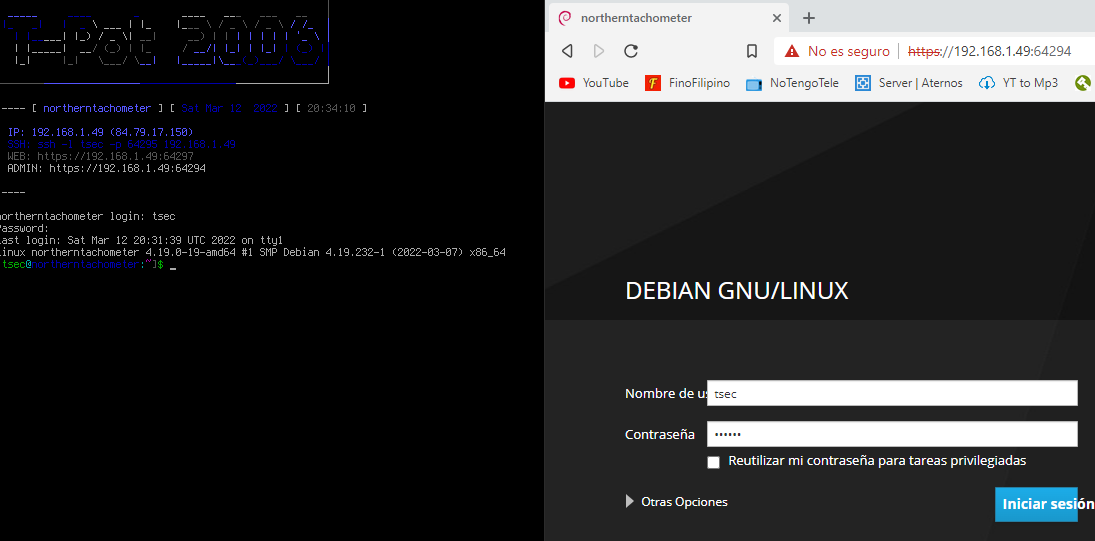
# **6. Configuración Red**

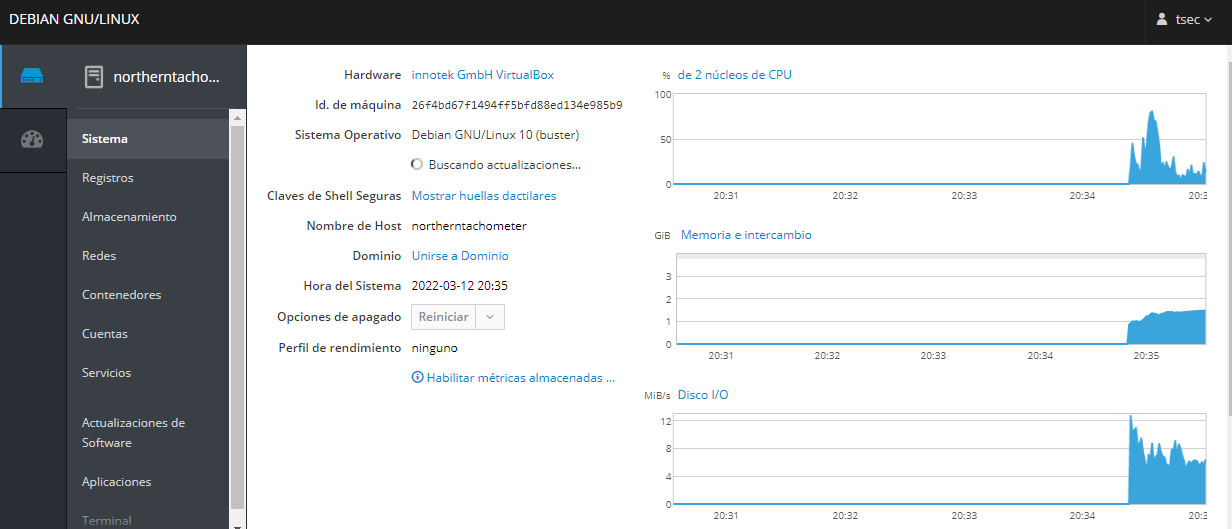
Para acceder via web a T-Pot debemos teclear la dirección web que aparece cuando arranca el sistema. Nos pedirá usuario y contraseña que pusimos en la instalación (si queremos establecer una IP fija utilizar /etc/network/interfaces)

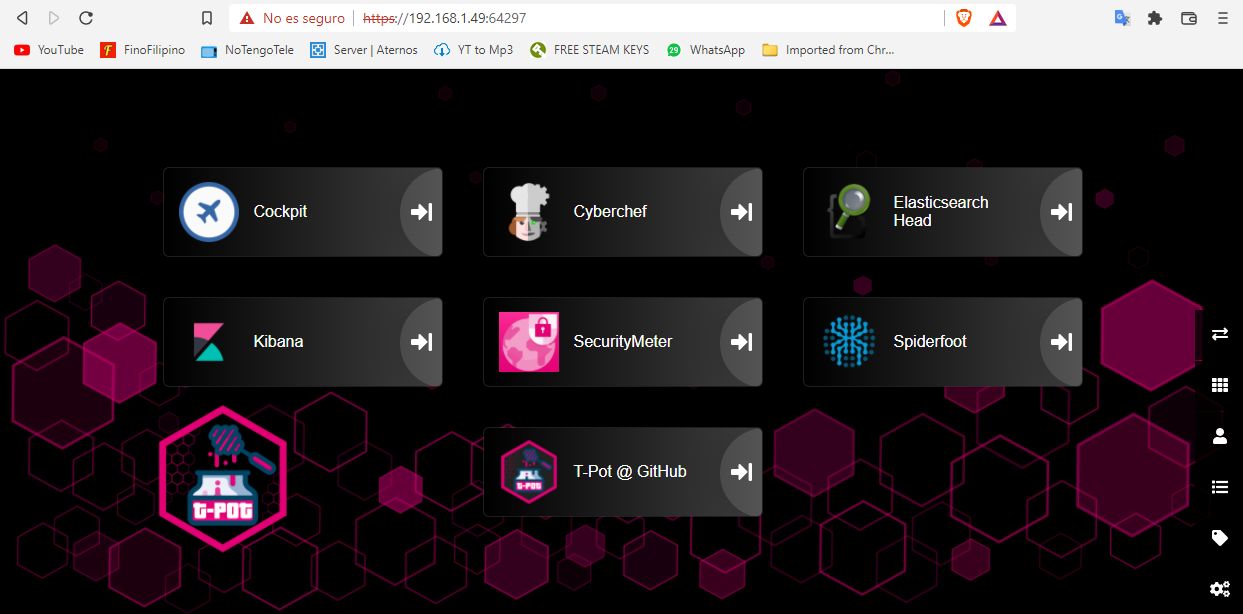


# **7. Configuración y Acceso Web**

En el panel de control de T-Pot acceder al apartado Cabina (cockpit) con el usuario y contraseña. Se puede marcar la casilla para que guarde la contraseña y no nos la solicite más.

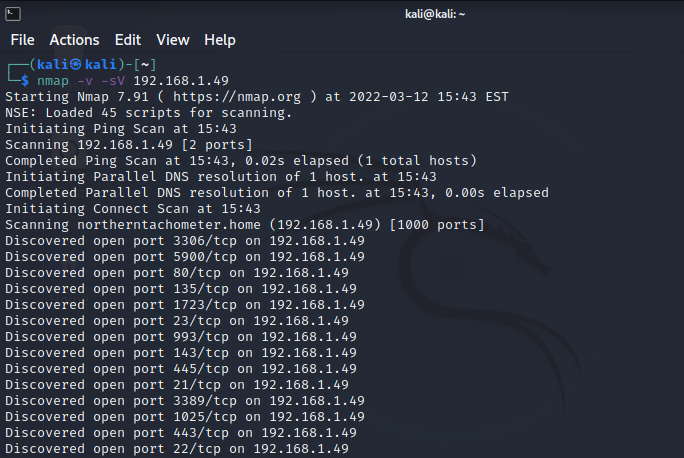


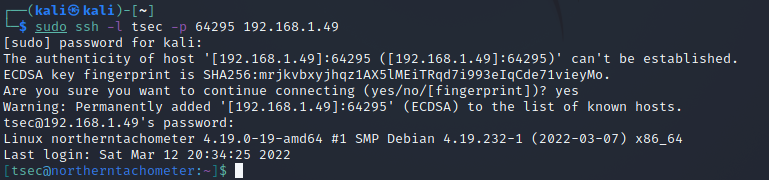




# **8. Escaneo de puertos y conexión SSH**

Realizar un escaneo para ver que puertos están abiertos nmap -v -sV IP\_máquina (encontrará más de 800 servicios con puertos abiertos). El servicio que nos interesa es el SSH.

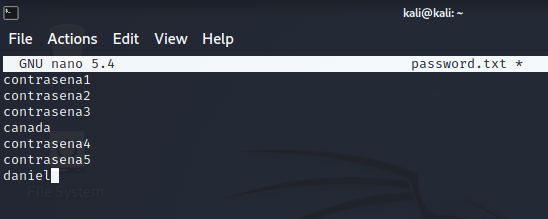




# **9. Ataque SSH**

Abrimos la MV Kali para realizar un sencillo ataque de fuerza bruta (diccionario) hacia nuestro servicio SSH. Como conocemos el usuario, la contraseña y la dirección IP del servidor que queremos atacar vamos a utilizarla, evidentemente esto en un entorno real no es así, la desconocemos y es mucho más complejo adivinarla.

En la máquina Kali, crear un fichero fichero de texto con el nombre password.txt en la ruta /home/kali Nos inventamos unas cuantas contraseñas y además añadir la que hemos puesto en la máquina T-Pot.



Abrir la consola de metasploit y seleccionar la herramienta ssh\_login para realizar un ataque de fuerza bruta con diccionario:

Utilizaremos los siguientes comandos:

use auxiliary/scanner/ssh/ssh\_login

set PASS\_FILE /home/kali/password.txt

set RHOSTS ip\_máquina\_atacar

set RPORT 22

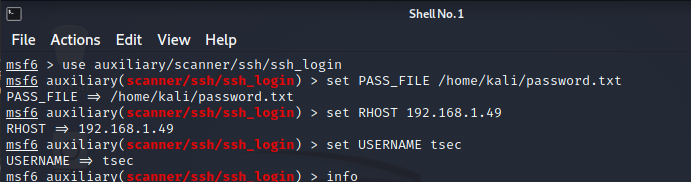
set USERNAME

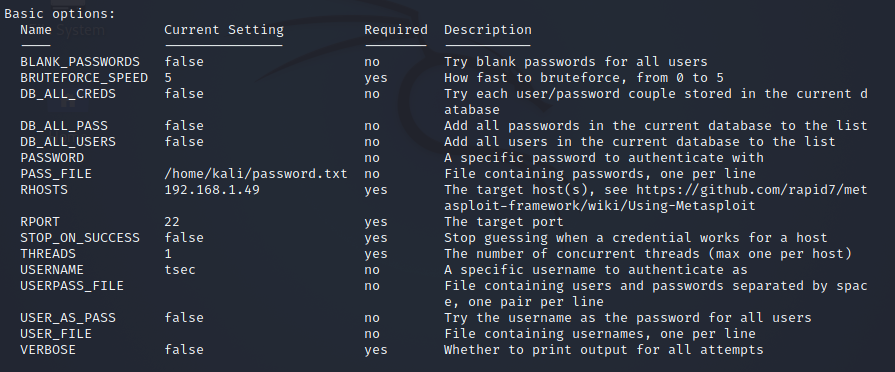
tsec (el usuario que supuestamente hemos descubierto que existe en el sistema)

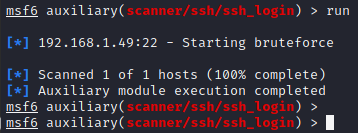
set VERBOSE true

info (se comprueba la información introducida)

run (ejecución del ataque)







Se pueden observar los ficheros de log de cowrie en nuestra máquina T-Pot. Para ello ir a la carpeta /data/cowrie/log/ y hacer un ls Observar dentro del fichero cowrie.json los diferentes intentos de contraseña del usuario tsec, junto con la IP del atacante y demás información.

