PRÁCTICA 4: HONEYPOT

INTRODUCCIÓN

Se denomina Honeypot al software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los **Honeypots** pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al **Honeypot.**

T-Pot se basa en una distribución Debian (Estable), con muchos demonios honeypot (todo-en-uno), así como otros componentes de soporte, incluidos en contenedores con Docker. Esto nos permite ejecutar múltiples demonios honeypot en la misma interfaz de red, manteniendo un pequeño espacio y restringiendo cada honeypot dentro de su propio entorno. Cada servicio de honeypot funciona detrás de un contenedor volátil para mayor seguridad, aunque los datos son guardados y mostrados visualmente en ELK (**Elasticsearch + Logstash + Kibana**) . Kibana permite a los usuarios visualizar los datos en cuadros y gráficos con Elasticsearch.

T-Pot es un desarrollo de código abierto que combina honeypots de baja y alta interacción en un único sistema. Su implementación es bastante sencilla y nos permite emular servicios de red como Android ADB, hardware de red vulnerable como routers, SCADA, SSH, Telnet, DICOM, Elasticsearch, FTP, RDP, HTTP/S, postgreSQL, MSSQL, POP3, SMTP, SMB, entre otros.

DESARROLLO DE LA PRÁCTICA

El objetivo de la práctica será crear un honeypot con la herramienta T-Pot. Para probarlo se realizará un ataque por fuerza bruta utilizando Metasploit, en concreto el módulo *ssh_login,* con el fin de ver cómo es la estructura del Honeypot una vez se ha conseguido el acceso (Cowrie).

1. Descargamos la ISO de T-Pot del siguiente repositorio:

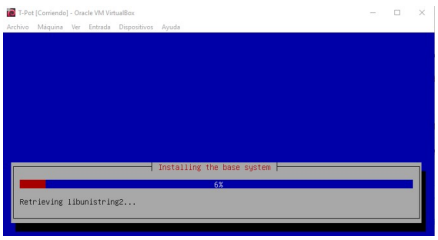
   https://github.com/telekom-security/tpotce/releases

   Comprobar la descarga mediante el archivo resumen SHA256.

2. 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)



Instalación

Standard. Honeypots: adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeysap, honeytrap, mailoney, medpot, rdpy, snare & tanner (8GB de ram)

Sensor. Honeypots: adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeypy, honeysap, honeytrap, mailoney, medpot, rdpy, snare & tanner (sólo requiere 4GB de RAM al no usar ELK)

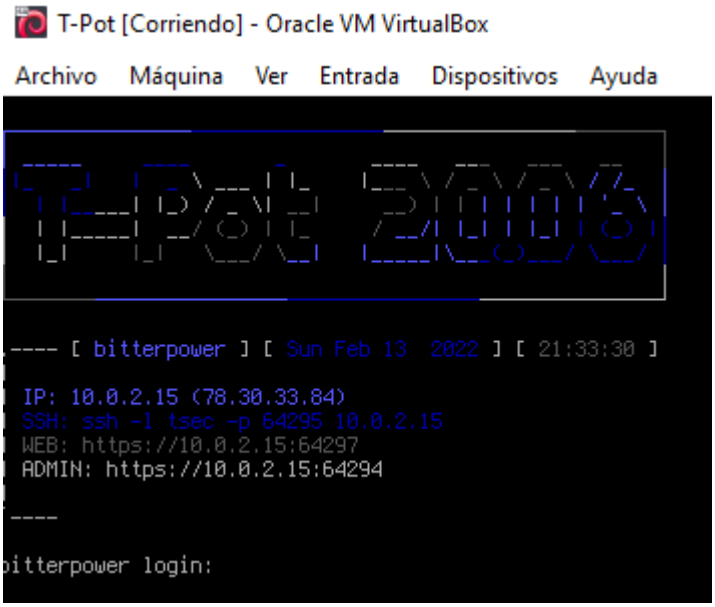
Industrial. Honeypots: conpot, cowrie, dicompot, heralding, honeysap, honeytrap, medpot & rdpy

Collector. Honeypots: heralding & honeytrap

Nextgen. adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, glutton, heralding, honeypy, honeysap, ipphoney, mailoney, medpot, rdpy, snare & tanner

Medical. dicompot & medpot

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



sudo su
cd *opt*/tpot
sudo ./update.sh -y

Si quisiéramos cambiar la versión en la que estamos (Standard, Sensor) podemos usar:

sudo *opt*/tpot/bin/tped.sh

Si quisiéramos controlar el servicio de tpot, usamos la orden:

sudo systemctl stop | start | status | restart

El fichero de configuración systemd se encuentra en:

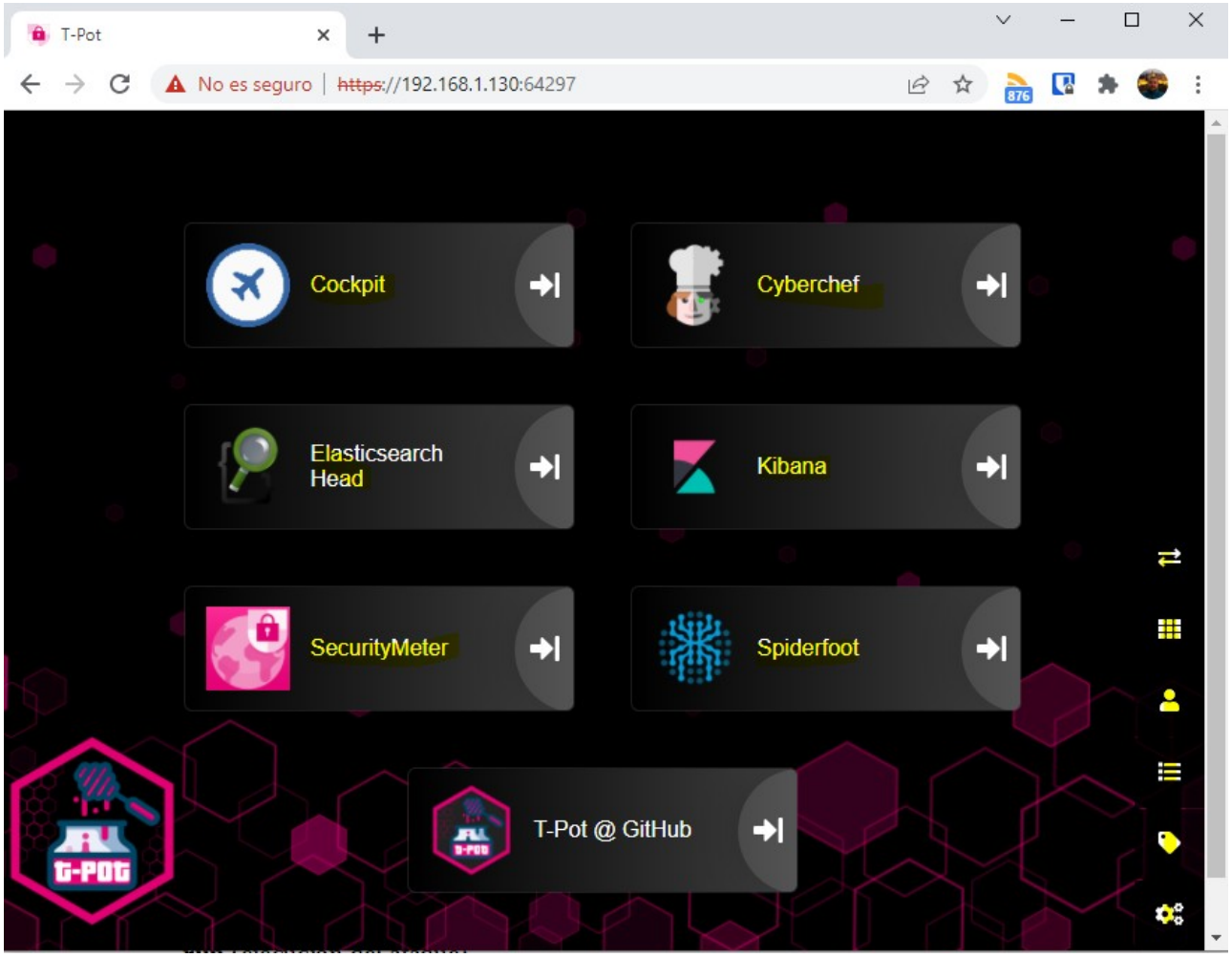
/*etc*/systemd/system/tpot.service

Para controlar el servicio de red debes usar:

sudo /*etc*/init.d/networking {status | stop | start}

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

5. 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**)



6. 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.
7. 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.

```
Completed Connect Scan at 10:38, 10.17s elapsed (1000 total ports)
Initiating Service scan at 10:38
Scanning 851 services on 192.168.1.130
Service scan Timing: About 1.52% done; ETC: 11:14 (0:35:37 remaining)
```

```
Service scan Timing: About 90.18% done; ETC: 10:49 (0:01:04 remaining)
Completed Service scan at 10:50, 712.58s elapsed (855 services on 1 host)
NSE: Script scanning 192.168.1.130.
Initiating NSE at 10:50
```

```
PS C:\Users\Samuel> ssh -p 64295 tsec@192.168.1.130
The authenticity of host '[192.168.1.130]:64295 ([192.168.1.130]:64295)' can't be established.
ECDSA key fingerprint is SHA256:tY7Z+nrH1xTjxDCibX2u+/eIkAfpQxuIvTmtdzwQh+o.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.1.130]:64295' (ECDSA) to the list of known hosts.
tsec@192.168.1.130's password:
Linux bitterpower 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64
Last login: Sun Feb 20 09:20:48 2022
[tsec@bitterpower: ]$ pwd
/home/tsec
[tsec@bitterpower: ]$
```

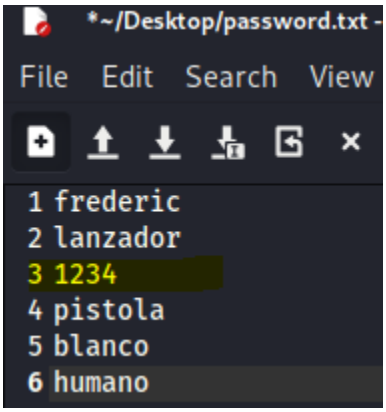
SSH para administración de T-POT

```
PS C:\Users\Samuel> ssh -p 22 profesor@192.168.1.133
Password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
profesor@ubuntu:~$ pwd
/home/profesor
profesor@ubuntu:~$
```

Servicio SSH a atacar

8. 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.

9. 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.



10. Abrir la consola de metasploit y seleccionar la herramienta **ssh_login** para realizar un ataque de fuerza bruta con diccionario:

    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)

    Debe encontrar la coincidencia porque hemos puesto la contraseña real en el fichero password.txt

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.1.133:22 - Starting bruteforce
[-] 192.168.1.133:22 - Failed: 'profesor:frederic'
[!] No active DB -- Credential data will not be saved!
[+] 192.168.1.133:22 - Success: 'profesor:lanzador' ''
[*] Command shell session 1 opened (192.168.1.135:44019 → 192.168.1.133:22) at 2022-03-06 10:42:33 -0500
```

11. Nos conectamos al servicio desde la misma consola usando:

    ssh -p 22 profesor@IP_máquina_atacar

    Teclear unos comandos cualquier para luego comprobar que queda registrado en T-pot (pwd, cat /*etc*/passwd)

12. En la máquina **T-Pot**, desde el panel de control, acceder al módulo **kibana** y luego a la opción **cowrie**. En el mapa se pueden ver los diferentes ataques que se han realizado. Deberá mostrarse que se realizado ataques ssh, con las IP's, comando que se han utilizado,…

    Se pueden también 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.

La máquina T-POT necesita bastantes recursos para funcionar adecuadamente. Sino logramos abrir Kibana, acceder al fichero log e interpretar la información del fichero cowrie.json

Solución o información:

https://blog.elhacker.net/2021/01/instalar-honeypot-t-pot-en-una-maquina-virtual-tpotce-cowrie-docker-dionea.html