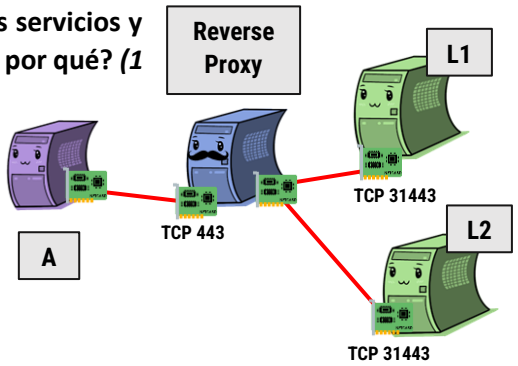
Seguridad de Sistemas Informáticos. Examen de Teoría Evaluación Ordinaria. Curso 2022-2023

Nombre:
UO:

NOTA: *Este examen mide tu capacidad para aplicar conocimientos teóricos de seguridad en un momento determinado, y en tus circunstancias actuales. No mide ni tu inteligencia ni tu habilidad general. ¡Confía en ti y a por ello!, pero si tienes un mal día, vendrán otros mejores.* ***NO te dejes hundir por un mal resultado***

1) **Mira el dibujo ¿Puede alguien desde la máquina A escanear los servicios y puertos de la máquina L1? ¿O solo los de otra máquina? ¿Cuál y por qué?** ***(1 punto)***



2) **¿Puedes explicar los pasos que darías para intentar comprometer la máquina que tenga esta salida de nmap?** ***(1 punto)***

```
admin@ip-172-26-0-73:~$ nmap -sV scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 03:00 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nombre:
UO:

3) **En tu trabajo te comentan que en el proyecto que estás trabajando hay alguna dependencia (librería, framework...) obsoleta y quizá con vulnerabilidades, pero que, como se están usando muchas dependencias, no es viable ni económico revisarlas a mano, por lo que no se va a hacer nada al respecto. ¿Crees que esto es cierto y que realmente no hay forma de automatizar su comprobación?** ***(1 punto)***

4) **¿Hay algún tipo de herramienta de seguridad que recomendarías en tu trabajo para detectar automáticamente si algún empleado está accediendo a máquinas a las que habitualmente no accede o en horas que están fuera de su horario laboral?** ***(1 punto)***

5) **Tu empresa ha contratado a un hacker experto, que informa que las máquinas son seguras porque, tras muchos intentos de ataque, no ha podido establecer ningún *bind shell* para controlar máquinas de la empresa. ¿Crees que tiene razón? ¿Crees que el tipo de shell que está intentando establecer es el correcto? En caso de que no, ¿Cuál recomendarías y por qué?** ***(1 punto)***

Nombre:
UO:

6) **Tu jefe te pide que implementes a mano un programa en *Python* que, al ejecutarse, establezca un *shell* a la máquina situada en la IP `192.168.12.3` en el puerto `3000` a mano. ¿Qué harías en lugar de codificarlo a mano para crearlo más rápido? ¿Qué tendrías que hacer en la máquina remota para que funcione? *(1 punto)***

7) **Se sospecha que un programa que estáis usando en el trabajo lee el portapapeles de forma fraudulenta, pero nadie sabe averiguarlo sin ejecutar el programa, algo que no podéis hacer por si es un *malware*. ¿Cómo comprobarías si efectivamente se está leyendo el portapapeles sin ejecutar el programa? (NOTA: Para leer el portapapeles hace falta llamar a funciones del API del kernel de *Windows*) *(1 punto)***

8) **Estás desarrollando una aplicación en la que los usuarios tienen que subir fotografías frecuentemente. ¿Qué política de seguridad en relación con las imágenes tendría tu aplicación para que estuviera más protegida frente a ataques? En caso de que la aplicación que estés desarrollando no utilice imágenes y los usuarios no tengan que subirlas, ¿cambiaría esta política? *(1 punto)***

Nombre:
UO:

9) **Un compañero tuyo está dudando entre usar *CSP* o *Strict-CSP* en las cabeceras HTTP de un proyecto de desarrollo web. ¿Podrías explicarle la diferencia entre los dos para ayudarle a tomar la decisión de cuál utilizar?. Comenta ventajas y desventajas de ambas *(1 punto)***

10) **Estás en un evento de la universidad que tiene como objetivo realizar un CTF (*Capture The Flag*), y te dan una máquina virtual que debes descomprimir y arrancar, pero no te dan más información de ella. ¿Cuál sería el primer paso que harías sobre la máquina? Imagina que llega un momento del evento en el que obtienes un usuario de la máquina, ¿cuál sería la próxima etapa o los próximos pasos a seguir? *(1 punto)***