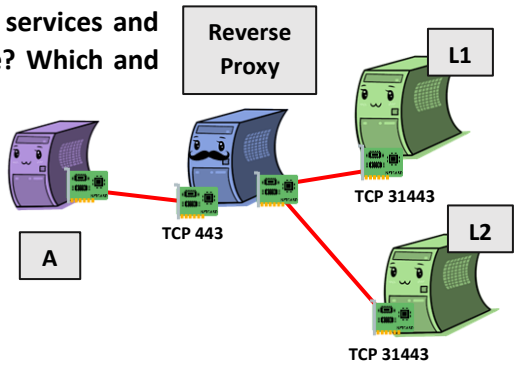
Computer Security. Theory Exam. Ordinary Evaluation 2022-2023

Name:
UO:

NOTE: *This exam measures your ability to apply theoretical security knowledge at a particular time, and in your current circumstances. It measures neither your intelligence nor your overall ability. Trust yourself and go for it!, but if you have a difficult day, better ones will come.* ***DO NOT let yourself be discouraged by a bad result.***

1) **Look at the drawing. Can someone from machine A scan the services and ports of machine L1? Or just the services of another machine? Which and why?** ***(1 point)***



2) **Can you explain the steps you would take to try to compromise the machine that has this nmap output?** ***(1 point)***

```
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
```

Name:
UO:

3) **Someone in your work tells you that the project you are working with might have some obsolete dependencies (libraries, frameworks…), that perhaps have vulnerabilities. However, the project uses too many dependencies, and it is not viable or economical to review them by hand, so nothing will be done about it. Do you think this is true and that there is no way to automate its verification?** ***(1 point)***

4) **Is there any type of security tool you can recommend in your work to automatically detect if an employee is accessing machines that they do not usually access or during hours that are outside of their working hours?** ***(1 point)***

5) **Your company hired an expert hacker, who reports that the machines are safe because, after many attack attempts, he has not been able to establish any *bind shell* to control company machines. Do you think he is right? Do you think the type of shell he is trying to establish is the right one? If not, which one would you recommend and why?** ***(1 point)***

Name:
UO:

6) **Your boss asks you to manually code a *Python* program that, when executed, sets a *shell* to a known machine located on IP 192.168.12.3 on port 3000 by hand. What would you do instead of manually coding it to create it faster? What would you have to do on the remote machine to make it work? *(1 point)***

7) **It is suspected that a program you are using at work reads the clipboard fraudulently, but nobody knows how to find out without running the program, something you cannot do in case it is *malware*. How would you check if the clipboard is actually being read without running the program? (NOTE: Reading the clipboard requires calling *Windows* kernel API functions) *(1 point)***

8) **You are developing an app where users have to upload photos frequently. What security policy would your app have for images to make it more protected from attacks? If the app you are developing does not use images, and users do not have to upload them, would you change this policy? *(1 point)***

Name:
UO:

9) **A colleague of yours is hesitating between using CSP or *Strict-CSP* in the HTTP headers of a web development project. Could you explain the difference between the two, so you can help him to decide which one to use?. Discuss advantages and disadvantages of both *(1 point)***

10) **You are at a university event that aims to perform a CTF (*Capture The Flag*), and they give you a virtual machine that you have to unzip and boot, but they do not give you more information about it. What would be the first step you would do on the machine? Imagine that there is a moment of the event when you get a user of the machine, what would be the next stage or the next steps to follow? *(1 point)***