Computer Security. Laboratory exam. Extraordinary call 2023

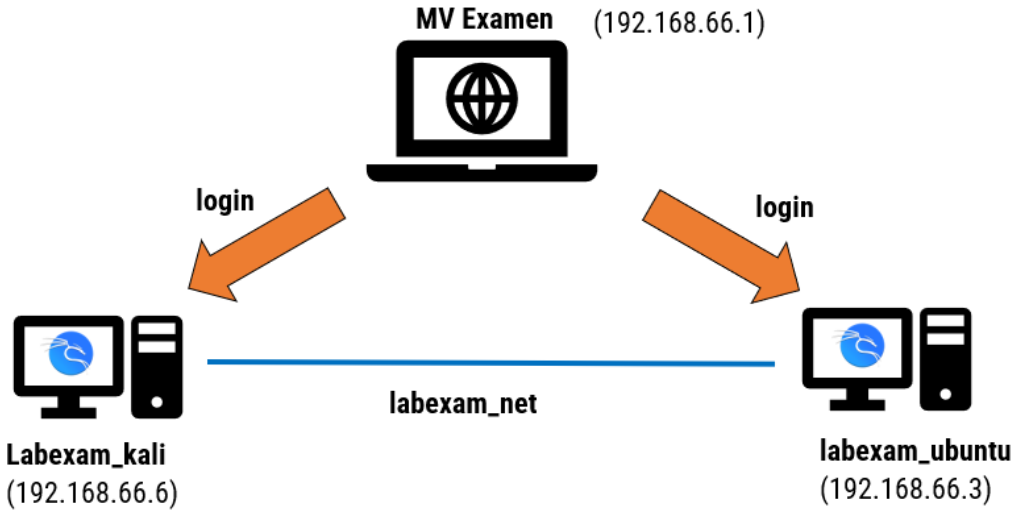
Full name:

UO:

NOTE: *This exam measures your ability to apply practical 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 bad day, better ones will come.* ***DO NOT be discouraged by a bad result***

Instructions:

The following diagram shows the infrastructure provided for this exam, consisting of **a VM identical to the one used in labs** with 2 containers (also like the ones you used).



To access them, on the desktop of the virtual machine you will see the `ssi_labs/lab_exam` folder. **This folder contains the laboratory that you will have to use in this exam, composed by:**

- A *Kali container* with MSF installed
- An *Ubuntu container* with some services running.

The containers are already built, so you just must **run `build_lab_exam.sh` to start the infrastructure** (**it is NOT NECESSARY to run `prepare_lab_exam.sh`**). As in the labs, you can log in to both with the `enter_kali_exam.sh` and `enter_ubuntu_exam.sh` scripts provided.

The IPs of the three components of our infrastructure are the ones that appear in the image. **Remember that you can bring all the materials developed in the laboratories to help you in this exam.**

Delivery:

You must submit **a single PDF file in** the task enabled in the virtual campus with the **necessary screenshots and explanations that show** that you have done each exercise. It is recommended to open a *Word file* from the beginning of the exam, and include screen captures and explanations as you complete exercises, saving often to avoid losing information. You can then **save the file as a PDF before delivering it to the virtual campus.**

Exercises:

1. ***(2 points)*** **Obtain a *Lynis* security score of the delivered VM (*Lynis* is already installed on it). Then, evaluate and remediate the Ubuntu OS of the VM according to the CIS profile contained on the zip file you can find in the `ssiuser` Desktop, using *SCAP Workbench* (already installed in the VM). Evaluate the VM with *Lynis* again to see if its score has changed. You must provide the initial and final *Lynis* score screenshot in the delivered PDF, along with the screenshot of *SCAP Workbench* configured prior to launch the scan.**

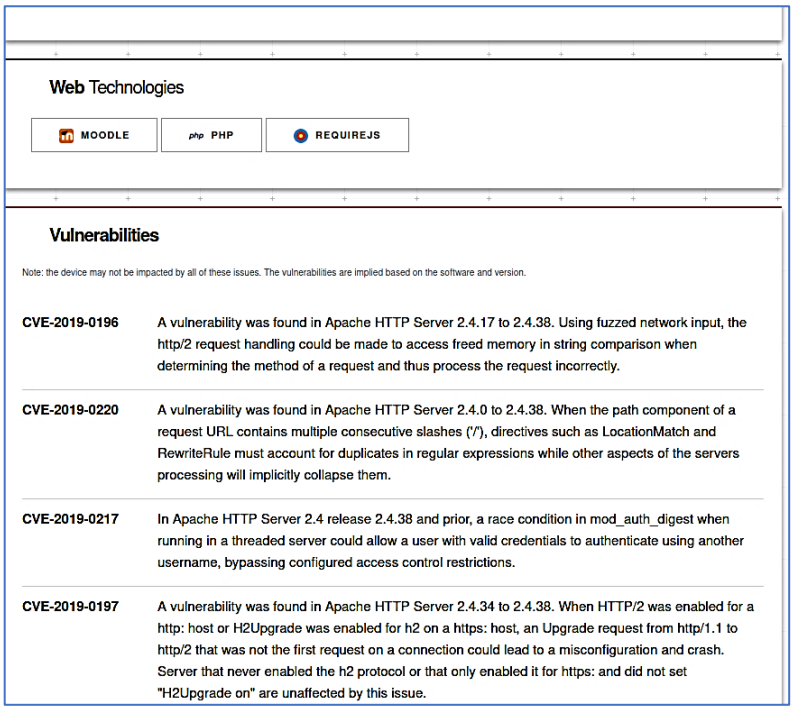
Computer Security. Laboratory exam. Extraordinary call 2023

Full name:

UO:

2. ***(1,5 points)*** **Read the complete metadata of the *CIS benchmark* file present on the `ssiuser` Desktop and include the screenshot on the results report. Then, delete all metadata of that file, and also show the resulting screenshot**.

3. ***(1,5 points)*** **Read and interpret this *Shodan* result, explaining the interesting things you see regarding security.**



4. ***(1,5 points)*** **Create a text file and encrypt it two times with two different passwords you choose, so to read the file again you must know both passwords, and decrypt with one password first, and then decrypt the result of this first decryption with the second one. Show the commands you used to do that and the decryption process in a screenshot.**

5. ***(2 points)*** **Perform a fast OS and service detection of the *Ubuntu* container from the VM using the appropriate tool. Then, detect the possible CVEs of the *Ubuntu* container from the VM again, choosing the correct features of the previous tool. Show two screenshots of the result of both operations**

6. ***(1,5 points)*** **Perform a reverse shell connection from the VM to the *Ubuntu* container using `ncat` and *Python*. Show the commands you used for that and screenshots with the resulting connections established.**