

Computer Security. Theory Exam January 2023

Name and Surname:

UO:

1) The company I have joined has been attacked, and I have been given a log of connections that I am sure has not been altered. On the date and time of the attack there is a huge number of connections of the IP 192.168.10.15, and the IT manager of my company tells me that it is a Russian IP. Do you think it's possible that this IP is from Russia? If you think it might be, how would you guess it? *(1 point)*

2) My boss authorizes me to do a nmap scan to my company's network and I find an http service on the port 59345 of one of the machines. I asked, but no one knows what it does there or to whom it belongs. What do you think it may be a reason for the existence of this mysterious http service? *(1 point)*

Computer Security. Theory Exam January 2023

Name and Surname:

UO:

3) Explain what I would have to do so that someone could send me encrypted messages that only I could read, based on the concepts of cryptography that we have seen in theory (1 point)

4) How would you verify that a software you have downloaded has not been altered since its author published it (assume that the author provides you with the necessary data to do so, the question is regarding the procedure to do it that you would follow) (1 point)

Computer Security. Theory Exam January 2023

Name and Surname:

UO:

5) An auditor has arrived to help us to implement ISO 27001 in our company, and you tell him that all the machines of the company have applied and verified all the security controls of the *CIS Benchmarks* corresponding to their OS. The auditor says that this is not useful to meet any criteria of the ISO 27001 standard, and that we have to start over. It's true? Why? (1 point)

6) In the SNI (*Secure Network Infrastructure*) proposed in class, what elements make up the intranet of administration? List and explain them in 2 lines maximum each (1 point)

Computer Security. Theory Exam January 2023

Name and Surname:

UO:

7) DMZ (*Demilitarized zone*). Explain what it is and what it is used for (1 point)

8) Authorization (*AuthZ*). What is it? Ways to implement it (1 point)

Computer Security. Theory Exam January 2023

Name and Surname:

UO:

9) SQL Injection. Explain what it is (1 point)

10) GTFOBins. Explain what they are and how they work (1 point)