

## Exame em Época Normal

Nome: \_\_\_\_\_ Nº: \_\_\_\_\_

**Nota:** As respostas incorretas resultam num valor negativo (redução percentual) da nota de cada ponto, cujo valor mínimo é zero.

- 1 (1 ponto) Classify each of the following events into a single layer in the 4-layers model. One answer per row and per column.

0.25 cada resposta correcta.

Events	Application	Transport	Network	Link
A message from your friend arrives and your chat application displays a pop-up notification.	●	○	○	○
A message arrives which states that you friend has closed the chat connection.	○	●	○	○
A message gets sent from your computer to your router.	○	○	○	●
A message gets sent from your computer to your router to Google's server	○	○	●	○

- 2 (1 ponto) You are sending data over Ethernet that's 4533 bytes long. How many Ethernet frames will this be? (Select one answer only).

1.0 única resposta correcta.

- 4 bytes of 1000 bytes, and 1 frame of 533 bytes.
- 3 frames of 1500 bytes, and 1 frame of 33 bytes.
- 1 frame of 4533 bytes.
- 3 frames of 1500 bytes, 1 frame of 33 bytes, and 13 bytes of padding.

- 3 (1 ponto) Select all correct statements.

0.5 cada resposta correcta. -0.5 cada resposta xxxx errada.

- Every router keeps track of all devices connected to the entire Internet to route packets.
- A device will usually keep the same IP address over its life-time.
- A device will usually keep the same MAC address over its life-time.
- A routed network must not have any loops or cycles.
- IP addresses can be used to implement geo-blocking, a technique where access to content is restricted based on the user's geographical location.

4 (1 ponto) Select all correct statements.

0.25 cada resposta correcta.

- `affe::16` contains as many IP addresses as `beef::16`.
- `192.168.0.4/32` contains exactly one IP address.
- hacking `127.0.0.1` and deleting all data on the machine is a bad idea.
- there are  $256 \times 256 = 65536$  unique IPv4 addresses that start with `192.68`.

5 (1 ponto) Select all correct statements.

0.5 cada resposta correcta. -0.5 cada resposta errada.

- ☐ to maximise the chances of reaching its destination, a packet should set the lowest possible hop limit.
- ☐ the destination IP address in an IP packet always points to the next router on the path.
- having multiple submarine cables is primarily a safety measure, not a security measure.
- many of today's protocols were developed for an Internet with very different threat models.

6 (1 ponto) You listen to a presentation about a new network protocol for online banking. After the talk, there is a lot of discussion going on. **Check all the remarks** that are relevant under the **Dolev-Yao** model.

1.0 única resposta correcta. -0.5 cada resposta errada.

- ☐ The bank runs Windows on their servers. This will be insecure.
- ☐ It looks nice, the NSA (National Security Agency) will break the encryption function and use this to spy on us.
- ☐ What happens if someone breaks into the bank's data center? They should use a blockchain instead!
- I don't think they properly protect against transaction replay.

7 (1 ponto) For their new blockchain-based cryptocurrency venture, FooBank's CTO wants to get rid of all that unwanted software code and build revolutionary high-speed banking protocol directly on top of IP packets. They propose the following protocol for money transfers between two different bank branches: **"I first send you a packet with information of the receiver, then a packet with information of the amount, and then a packet with information of the recipient. Trust me, it's the best protocol we ever had!"**.

What could possibly go wrong? Select all correct statements.

0.25 cada resposta correcta.

- Some transfers may inexplicably fail.
- Instead of sending money from Alice to Bob, FooBank may end up sending money from Bob to Alice.
- Mischievous attackers may get rich.
- Someone in Russia may get wind of it.

8 (1 ponto) Your device has joined a new network that uses DHCP to assign you an IP address. What is the first thing that happens to get your new IP address? Select all correct statements.

1.0 única resposta correcta. -0.5 cada resposta errada.

- ☐ Your device asks for an IP address directly from the DHCP server.
- ☒ Your device broadcasts a DHCP request to all the clients on the network.
- ☐ The DHCP server sends an announcement and your client responds.
- ☐ Santa gets your request, checks his list and grants an address depending on whether your devices has been bad or good.

**9 (1 ponto)** What is UDP good for? Select all correct statements.

0.5 cada resposta correcta. -0.5 cada resposta errada.

- ☒ audio chat.
- ☐ sending emails.
- ☒ video chat.
- ☐ downloading web pages.
- ☒ real time systems.

**10 (1 ponto)** Who is the intended target of a reflection attack? Select all correct statements.

1.0 única resposta correcta. -1.0 cada resposta errada.

- ☐ the device the attacker is sending the request to.
- ☒ the device that is mentioned in the source IP field.
- ☐ the device the attacker is using to send packets.

## Parte II (5 pontos)

Durante a semana 11 de aulas estivemos á discutir sobre a TLS (segurança da camada de transferência), as autoridades certificadoras (certificate authorities), e sobre o role da criptografia no processo de segurança dos dados que são enviados a través de um navegador. **Estabeleça um símile (uma comparação) entre a segurança usada pela a TLS e o processo de notariação de documentos que é levado a cabo em cartórios notariais, tal como seguidamente explicado. O símile deve mapear e comparar elementos constituintes (integrantes) do mecanismo de segurança utilizados pela TLS com elementos constituintes do proceso de notariação, conforme explicado abaixo.**

A notariação de documentos é um processo legal que garante a autenticidade e a validade legal de documentos importantes, como contratos, procurações, testamentos, declarações juramentadas, entre outros. Esse processo é realizado por um notário público, sendo um profissional licenciado pelo Estado para autenticar documentos e certificar que as assinaturas são válidas. Os documentos são notariados essencialmente, por razões de segurança, credibilidade e legalidade jurídica. A notariação de documentos evita, por exemplo, que depois o outro interveniente venha dizer que a sua assinatura tenha sido falsificada. Noutras situações, é a própria lei que exige uma determinada formalidade, por exemplo, a compra e venda de bem imóvel exige uma notariação, sob pena de o acto (a venda do imóvel) não ter qualquer validade. Os actos notariais são praticados em cartórios notariais. Os cartórios notariais são competentes dentro do concelho ao que pertencem.

Durante o processo de notariação (autenticação), o documento é carimbado em cada página e um selo branco em relevo é colocado na última página ao pé onde o notário assina como garantia de autenticidade do documento. Os dois (ou mais) intervenientes no acto notarial devem rubricar cada página e assinar a última folha.

A Ordem dos Notários é a ordem profissional que regula, em parceria com o Ministério da Justiça, o exercício da atividade notarial em Portugal. A Ordem dos Notários é uma entidade independente dos órgãos do Estado, que goza de personalidade jurídica, e que representa os notários portugueses. O exercício da actividade notarial depende da inscrição na Ordem, inscrição que apenas é possível por parte de quem tenha obtido o título de notário.

**Resposta á Parte II.**

### Parte III (5 pontos)

- 1 (1 ponto) What happens when an application takes user inputted data and sends it to a web browser without proper validation and escaping? Select all correct statements.

1.0 única resposta certa. -0.5 cada resposta errada.

- ☒ Cross Site Scripting
- ☐ Security Misconfiguration
- ☐ Broken Authentication and Session Management

- 2 (1 ponto) Which of the following statements are correct? Select all correct statements.

1.0 única resposta certa. -0.5 cada resposta errada.

- ☐ For a secure application, it is sufficient to use HTTPS for the login pages only.
- ☒ Using a secure flag in the session cookie stops the cookie from being transmitted over HTTP.
- ☐ SQL injection can be stopped by not showing the error messages back to the user.

- 3 (1 ponto) Your application sets a cookie with Secure attribute. What does this mean? Select all correct statements.

1.0 única resposta certa. -0.5 cada resposta errada.

- ☐ The cookie cannot be accessed by JavaScript
- ☐ The cookie will not be sent cross-domain
- ☒ Client will send the cookie only over an HTTPS connection

- 4 (1 ponto) What is the type of flaw that occurs when untrusted user-entered data is sent to the interpreter as part of a query or command? Select all correct statements.

1.0 única resposta certa. -0.5 cada resposta errada.

- ☐ Insecure Direct Object References
- ☒ Injection
- ☐ Insufficient Transport Layer Protection
- ☐ Cross Site Request Forgery

- 5 (1 ponto) Why is sending session ID in the GET parameters of the URL bad from a security perspective even on a site that is served completely over HTTPS? Select all correct statements.

1.0 única resposta certa. -0.5 cada resposta errada.

- ☐ It is not bad, if the site uses HTTPS, it's all encrypted
- ☒ It is bad; session IDs might be visible in HTTP referrer header in logs of the third party sites or logs of web servers
- ☐ It is bad; attackers can sniff it, crack encryption and then see the session ID in the URL
- ☐ It not bad because session ID is a long string, so what if someone steals it