

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.

Parte I (10 pontos)

1 (1 ponto) Select all application types where UDP is more suitable than TCP.

1.0 única resposta certa. -0.5 cada resposta errada.

- ☒ video chat.
- ☐ on-demand video streaming.
- ☐ social media websites.

2 (1 ponto) What attributes of UDP contributes to it being used for amplification attacks? Select all correct statements.

0.5 cada resposta certa. -0.5 cada resposta errada.

- ☒ Connectionless.
- ☒ Spoofable.
- ☐ Guaranteed delivery.

3 (1 ponto) Which of the following items are some of the benefits of DNS. Select all correct statements.

0.33 cada resposta certa. -0.5 cada resposta errada.

- ☒ Ease of management.
- ☒ Availability.
- ☒ Human readable.
- ☐ Centralised repository of domain names.

4 (1 ponto) Assume that the **example.com** website includes 4 images, 2 links to other websites, and a reference to a stylesheet that formats the page contents. How many HTTP requests does a browser make when you write **example.com** in the address bar (and press enter)?

1.0 única resposta certa. -1.0 cada resposta errada.

- ☐ 4.
- ☐ 5.
- ☒ 6.
- ☐ 7.
- ☐ 8.

- 5 (1 ponto) Which of the following URLs would produce the same network activity as `http://example.com/?`
Select all correct statements.

0.33 cada resposta certa. -0.5 cada resposta errada.

- ☒ `example.com/`
- ☐ `http://example.org/`
- ☒ `https://example.com/`
- ☐ `http://example.com/#about`
- ☒ `http://example.com/?lang=en`

- 6 (1 ponto) What happens when you delete all your browser cookies? Select all correct answers.

1.0 única resposta certa. -0.5 cada resposta errada.

- ☒ You will be logged out of all of your website sessions.
- ☐ You will delete any traces you left on the Internet.
- ☐ Your Internet Service Provider will be unable to see which websites you are visiting.

- 7 (1 ponto) Which of the following URLs would (when entered into the address bar) produce the same network activity as `http://example.com/?` Select all correct answers.

0.33 cada resposta certa. -0.5 cada resposta errada.

- ☒ `example.com`
- ☐ `http://example.org/`
- ☒ `http://example.com:80/`
- ☐ `http://example.com/`
- ☒ `http://example.com/#about`
- ☐ `http://example.com/?lang=en`

- 8 (1 ponto) Take a look at the source code for the `dogs.example.com` page below. Assuming all machines speak HTTP/2, how many TCP connections need to be opened to display the page?

1.0 única resposta certa. -1.0 cada resposta errada.

```
<html>
  <head></head>
  <body>
    <h1> Pictures of Dogs </h1>
    
    
    
  </body>
</html>
```

- ☐ 1
- ☒ 2
- ☐ 3
- ☐ 4

- 9 (1 ponto) Assume Alice and Bob securely communicate over TLS. Mallory controls the network. What can Mallory do? Select all correct answers.

0.5 cada resposta certa. -0.5 cada resposta errada.

- Mallory can see who is communicating with whom.
- Mallory can secretly modify messages between Alice and Bob.
- Mallory can block the communication between Alice and Bob.
- Mallory can impersonate Bob.

10 (1 ponto) Select all correct answers about TLS.

0.5 cada resposta certa. -0.25 cada resposta errada xxxxx.

- TLS makes it possible to reduce the trusted areas while maintaining protection goals.
- Large parts of the Internet are using SSL version 3.
- When visiting Facebook, a browser (a client) proves its identity by presenting a TLS certificate.
- TLS cryptography is a solved problem.
- A website is trustworthy if it has a valid certificate.
- TLS does not protect against attacks on availability.

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) Which of the following are input validation vulnerabilities? Select all correct statements.

0.5 cada resposta certa. -0.5 única resposta errada.

- ☒ Cross-Site Scripting
- ☒ SQL Injection
- ☐ Session ID Disclosure in URL GET request.

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