
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) Select all correct statements.

- ☐ the router modifies the ethernet header before forwarding a packet.
- ☐ the TCP header contains the packet's destination IP address.
- ☐ to forward a packet, the router needs to parse the packet's TCP header.
- ☐ your ISP can read your packets when checking your network.

2 (1 ponto) The uniqueness of MAC addresses means they can be used as a form of access control, e.g., restricting access by MAC address to wireless networks.

- ☐ This is effective to prevent an attacker from joining the network.
- ☐ This is not effective to prevent an attacker from joining the network.

3 (1 ponto) Select all correct statements.

- ☐ 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.

- ☐ IP packets have a fixed length.
- ☐ The IP packet header is **sandwiched** between the link and the transport layers.
- ☐ IPv6 packets contain the destination's MAC address and the destination address.
- ☐ IP packets define the transport layer protocol used in the payload.

5 (1 ponto) Select all correct statements.

- ☐ 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) For each network attacker capability, which CIA goal is directly violated? **Check only one capability per row.**

Attacker Capability	Confidentiality	Integrity	Availability
Observe packets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Modify packets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Drop packets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Delay packets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forge packets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Replay packets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7 (1 ponto) Check all statements that are true about BGPs.

- ☐ The confidentiality of our communications can be asserted by physically protecting all fiber cables (in the world) on the default path.
- ☐ Securing BGP communications **today** is mostly an **afterthought** due to the fact that threat models have changed from the old Arpanet to the modern Internet.
- ☐ When leaving a spouse (home), one should reconfigure their BGP routes to protect her against stalking.

8 (1 ponto) Which statements are true about DHCP spoofing? Select all the correct statements.

- ☐ a client fools the DHCP server into giving it an IP address when it is unauthorised.
- ☐ an imposter DHCP server fools the client into thinking it is the real DHCP server.

9 (1 ponto) What do we need a port for? Select all correct statements.

- ☐ to uniquely identify a socket.
- ☐ to uniquely identify a device.
- ☐ to uniquely identify a program.
- ☐ to dock your ships.

10 (1 ponto) Select all application types where UDP is more suitable than TCP.

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

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 notarização 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 notarização, conforme explicado abaixo.**

A notarização 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 notarizados essencialmente, por razões de segurança, credibilidade e legalidade jurídica. A notarização 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 notarização, 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 notarização (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) Qual a melhor forma de realizar a validação de entrada do utilizador?
- ☐ Whitelisting
 - ☐ Blacklisting
- 2 (1 ponto) Qual o ataque que pode executar scripts no browser do utilizador e é capaz de sequestrar sessões de utilizadores, desfigurar sites ou redireccionando o utilizador para sites maliciosos? Selecione todas as afirmações corretas.
- ☐ Cross site scripting
 - ☐ Malware Uploading
 - ☐ Man in the middle
 - ☐ SQL Injection
- 3 (1 ponto) A sua aplicação define um cookie com um atributo de segurança. O que é que isto significa? Selecione todas as afirmações corretas.
- ☐ 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) Qual é o tipo de falha que ocorre quando dados não fidedignos introduzidos pelo utilizador são enviados para o intérprete como parte de uma consulta ou comando? Selecione todas as afirmações corretas.
- ☐ Insecure Direct Object References
 - ☐ Injection
 - ☐ Insufficient Transport Layer Protection
 - ☐ Cross Site Request Forgery
- 5 (1 ponto) O que acontece quando uma aplicação recolhe dados introduzidos pelo utilizador e os envia para um navegador sem a devida validação e “escaping”? Selecione todas as afirmações corretas.
- ☐ Cross Site Scripting
 - ☐ Security Misconfiguration
 - ☐ Broken Authentication and Session Management