



## Exame Isi

Lexislación e Seguridade Informática (Universidade da Coruña)

Correxido por  
Pericles 2023

## **EXAMEN LSI – ENERO 2017**

- 1) Según el Derecho comunitario un servicio de la sociedad de información es...
  - a) un servicio prestado a cambio de remuneración (no abarca servicios gratuitos) y por vía electrónica.
  - b) Un servicio prestado siempre a cambio de una remuneración, a distancia, por vía electrónica y, de forma habitual, a petición individual del destinatario del servicio.
  - c) Un servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual del destinatario del servicio.
  - d) Un servicio prestado por medios electrónicos, con independencia de otras características (puede ser remunerado o gratuito, a distancia o no, a petición individual o punto-multipunto).
- 2) De acuerdo con el art. 13 del Reglamento de la Ley Orgánica de Protección de Datos Personales...
  - a) Para el tratamiento de datos de menores de 18 años o más, se precisa siempre el consentimiento de los padres o representantes legales.
  - b) Para el tratamiento de dato de menores de 16 años o más, se precisa siempre el consentimiento de los padres o representantes legales.
  - c) Para el tratamiento de datos de menores de 14 años o más, se precisa siempre el consentimiento de los padres o representantes legales.
  - d) Para el tratamiento de datos especialmente protegidos de menores de 16 años o más, se precisa siempre el consentimiento de los padres o representantes legales.
- 3) El documento nacional de identidad electrónico permite la firma electrónica de documentos con la consideración...
  - a) De firma electrónica avanzada que equivale a la manuscrita.
  - b) De firma electrónica a secas.
  - c) De firma electrónica reconocida que equivale a la manuscrita.
  - d) De firma electrónica reconocida cuando lo reconoce el juez, siendo de este modo equivalente a la manuscrita.
- 4) El consentimiento en materia de protección de datos...
  - a) Es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. El consentimiento no puede ser tácito.
  - b) Se exigirá siempre al titular de los datos, con la única excepción de las fuentes de acceso al público (FAP), es decir, aquellos ficheros cuya consulta puede ser realizada por cualquier persona.
  - c) Es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. El consentimiento puede ser tácito.
  - d) No es válido cuando lo realiza un menor de 18 años. Se precisa siempre el consentimiento de sus padres o representantes legales.

- 5) La Comunidad Europea y España han optado por un mismo sistema para regular las comunicaciones comerciales electrónicas, ¿cuál es?
- a) El sistema opt out, que autoriza todas las comunicaciones comerciales electrónicas, aún sin consentimiento previo del destinatario.
  - b) El sistema opt in, que prohíbe sin excepción el envío de comunicaciones comerciales electrónicas cuando no hubieran sido solicitadas o expresamente autorizadas por los destinatarios con carácter previo.
  - c) El sistema opt out, que autoriza todas las comunicaciones comerciales electrónicas, aún sin consentimiento previo del destinatario, siempre que conste la palabra "publicidad" al comienzo del mensaje.
  - d) El sistema opt in, que prohíbe las comunicaciones comerciales electrónicas cuando no hubieran sido solicitadas o expresamente autorizadas por los destinatarios con carácter previo, con la excepción de que exista una relación contractual previa.
- 6) El tratamiento de datos especialmente requiere que el consentimiento del titular de los datos sea:
- a) Otorgado de manera expresa o tácita.
  - b) Otorgado de manera expresa.
  - c) Otorgado de forma expresa y en presencia de un notario.
  - d) Otorgado de manera expresa únicamente para los datos referidos a la identidad étnica y de manera tácita para el resto de datos especialmente protegidos.
- 7) De acuerdo con la Ley 34/2002, de 11 julio de servicios de la sociedad de la información y el comercio electrónico, ¿dónde se entiende celebrado un contrato electrónico en que interviene un consumidor (B2C)?
- a) En el lugar pactado en el contrato.
  - b) En el lugar donde se realiza la oferta.
  - c) En el lugar de establecimiento del prestador de servicios.
  - d) En el lugar de residencia habitual del consumidor.
- 8) ¿El Derecho español exige una forma concreta para la validez de los contratos?
- a) Sí. Los contratos han de llevarse a cabo por escrito para ser válidos. Los contratos llevados a cabo por medios electrónicos son inválidos, con la excepción de aquellos llevados a cabo mediante firma electrónica.
  - b) No. Rige el llamado "principio espiritualista" o de libertad de forma de los contratos. Y de acuerdo con este principio los contratos celebrados en forma electrónica son válidos.
  - c) Sí. Los contratos han de llevarse a cabo por escrito para ser válidos. Los contratos llevados a cabo por medios electrónicos son inválidos en principio, salvo que un juez los declare válidos.
  - d) No. Rige el llamado "principio espiritualista" o de libertad de forma de los contratos. Además, en muchos contratos no es necesario el consentimiento de las partes para que sean válidos.

9) 21

- a) Raíz cuadrada de 484 441
- b) Ssh 22
- ☒ c) ftp 21
- d) telnet 23

10) En el contexto de la seguridad informática, el código CVE-2014-0160...

- a) Se refiere a un conocido plugin para ettercap.
- b) Es un código de verificación electrónica.
- c) Es un algoritmo de hash o resumen.
- ☒ d) Identifica unívocamente una vulnerabilidad. Literalmente la V de CVE es de vulnerabilidad  
Direct attack -> ataca directamente una vulnerabilidad




11) Slowloris

- a) Direct attack que afecta a todos los servidores web.
- b) Reflective attack que afecta a todos los servidores web.
- ☒ c) Direct attack que afecta a algunos servidores web. Afecta a los que procesan conexiones concurrentes 1 a 1
- d) Reflective attack que afecta a algunos servidores web.

12) Nsswitch.conf

- a) Este archivo nos permite definir múltiples configuraciones de red para poder conectar nuestros equipos en diferentes redes. Suele utilizarse en quipos con movilidad entre redes domésticas y de trabajo.
- ☒ b) Este archivo nos permite configurar dónde buscar cierto tipo de información administrativa (hosts, passwd, group, shadow, networks...) Es literalmente su definicion wtf
- c) Este archivo únicamente se localiza en aquellos equipos que tienen conectividad mediante redes de medio conmutado, como las debían del laboratorio de prácticas, y se utiliza para la gestión de la paquetería de red.
- d) Ninguna de las anteriores es correcta.

13) DMZ

-  Intranet.
-  Outtranet.
- ☒ c) Red perimetral.
-  Red Privada Virtual. VPN

Una red perimetral actua como zona intermedia entre la red interna y la externa (intranet), aloja servicios que deben ser accesibles desde el exterior, pero sirve como una primera capa de defensa

14) Ataque LAND

- ☒ a) Generación de paquetes con origen y destino la misma máquina, para que los auto-respondan. Literalmente este wtf
- b) Generación de paquetes con origen la máquina a atacar y destino una dirección de broadcast, para conseguir un factor de amplificación alto.
- c) Generación de paquetes con origen una dirección de broadcast y destino la máquina a atacar.
- d) No existe tal tipo de ataque.



- 15) En un certificado digital emitido para un servidor web, el campo CN (Common Name) del certificado...
- a) Debe contener el nombre y apellidos del responsable del sitio Web.
  - b) Debe contener una dirección de correo electrónico de contacto (p. ej: [info@udc.es](mailto:info@udc.es))
  - ☒ c) Debe coincidir con el nombre del sitio web (p. ej: [www.udc.es](http://www.udc.es)) [Nombre del dominio completo](#)
  - d) Debe contener el nombre de la autoridad certificadora que emite dicho certificado.

- 16) OWASP TOP 10 del 2013 en tercera posición:

- a) Password guessing.
- ☒ b) Cross-Site Scripting. [Curiosidad profe , en 2022 en 3º puesto estuvo Exposición de Datos Sensibles](#)
- c) DoS.
- d) Buffer Overflow.

- 17) NDP utiliza

- ☒ a) Paquetes ARPv4 [NDP es IPv6](#)
- b) Paquetes ARPv6 [Literalmente el NDP es el ARP de IPv6 wtf](#)
- ☒ c) Paquetes ICMPv4 [Idem a\)](#)
- ☒ d) Paquetes ICMPv6

- 18) HTTP\_X\_FORWARDED\_FOR

- ☒ a) No tiene relevancia en el ámbito de la privacidad y el anonimato.
- ☒ b) Únicamente incluye el nombre o dirección IP del servidor web. [Pa empezar, añade una IP extra](#)
- ☒ c) Si no está vacío denota el uso de un proxy. [O balanceador de carga por lo que he visto, pero kk](#)
- d) Se utiliza para hacer forwarding a nivel IP.

- 19) Los TCP Wrappers

- ☒ a) Filtran todos los servicios de red de nuestros sistemas. [Tanto TCP como UDP](#)
- ☒ b) Filtran todos los servicios TCP de nuestros sistemas. [La información nos dice que están hechos para TCP pero técnicamente no se limitan a TCP. También hacen distinción entre TCP wrappers y hosts.allow y hosts.deny. Se acepta la duda de que puede ser la b\)](#)
- c) Trabajan a nivel de kernel.
- d) Ninguna de las anteriores es correcta.

- 20) Considerando como referencia la red de prácticas, en la máquina 10.10.102.200 se configura arpon de forma estática. En la 10.10.102.199 se hace un MITM por arp spoofing de tipo remote entre la 10.10.102.200 y el "router". Desde la 10.10.102.200 "navegamos" a distintas páginas web.

- a) La 10.10.102.199 captura la totalidad de la paquetería de navegación de la 10.10.102.200 dado que arpon detecta el ARP spoofing pero no protege.
- ☒ b) La 10.10.102.199 no captura ningún tráfico de la navegación web. [Arpon impide que cambie la MAC del router por la de la 199](#)
- c) La 10.10.102.199 capturarán una parte de la paquetería de la navegación.
- d) La 10.10.102.199 quedará bloqueada y se le producirá una denegación de servicio por la acción de arpon.

[A que cojones se refiere con esto, hombre Arpon no me va a hacer un puñetero DoS si me intento conectar en el medio, bloquear en sí tampoco me bloqueará, pero no voy a estar muy In The Middle](#)

- 21) SHA3

- ☒ a) Keccak [Curiosidad profe, de hecho Keccak es el nombre del diseño original y SHA3 el estándar basado en ese diseño](#)
- ☒ b) AES [AES sirve para cifrado simétrico y SHA3 para funciones de hash criptográficas](#)
- ☒ c) X509 [Esta es para gestión y verificación de certificados digitales](#)
- d) Sniffing

22) 802.1x

- a) Estándar que define un formato de certificado digital.
- b) Estándar para prevenir el DHCP spoofing.
- c) Estándar que permite a múltiples redes compartir el mismo medio físico.
- d) Estándar para el control de acceso a red.**

Proporciona un marco de autenticación de dispositivos que intentan conectarse a una red

23) Un paquete SYN a un puerto abierto recibirá

- a) Un SYN
- b) Un SYN-ACK**
- c) Un ACK
- d) Ninguna de las anteriores es correcta.

Cliente	Servidor
-----	
SYN	
	SYN-ACK
ACK	

24) Desde su máquina virtual (1010.102.XX), en el entorno de prácticas del laboratorio, ejecuta, como usuario privilegiado el siguiente comando: #nmap -sP 10.10.102.27

- a) Nmap efectuará "host Discovery"** Hace pings
- b) Nmap efectuará "port Scanning" -p es la flag para port scanning
- c) Nmap efectuará "host Discovery" y, si la máquina está "viva", efectuará "port scanning". Coño, si no tiene la flag -p, pues no, eso es de 1º de nmap
- d) Nmap efectuará "fingerprinting". ???

25) El anonimato que proporciona la red Tor se basa en...

- a) Usar cifrado extremo-a-extremo (desde la máquina del usuario hasta la máquina de destino).
- b) Usar una red paralela a Internet, con infraestructura propia.
- c) Ocultar la identidad de los nodos intermedios.**
- d) Ninguna de las anteriores.

26) Un ataque de tipo CAM flooding...

Entra en modo aprendizaje

- a) Se basa en llenar la tabla CAM del switch, para que éste se comporte como un hub.
- b) No funcionará si los usuarios han configurado mapeado ARP estático en sus equipos.**
- c) Es un ataque de tipo MITM. NO
- d) Se basa en asociar la dirección MAC del atacante con la dirección IP del switch y así recibir todo el tráfico que pasa por el switch.

Efectivamente, así no aprende dinámicamente

27) SYN-COOKIES...

- a) Son una protección contra DoS que consiste en emplear una estructura de datos independiente y paralela a la Transmission Control Block para evitar la sobrecarga de esta última.
- b) Son una protección contra DoS que se basa en utilizar el número de secuencia TCP para codificar datos y así reservar espacio para la conexión únicamente cuando se recibe el mensaje de confirmación final.** Si hombre, si hombre literalmente es esta
- c) Son una protección contra la captura de sesiones SSL a través del empleo de Cookies en un ataque MITM.
- d) Son una protección contra DoS que consiste en almacenar en una cookie datos identificativos de los clientes, para saber quién está generando el ataque.



28) En su máquina de laboratorio, desde una consola, con permisos de root, usted ejecuta:  
`#iptables -P INPUT DROP; iptables -F`

¿Qué sucederá entonces?

a) Se borrarán todas las reglas de INPUT y se listarán las reglas por pantalla.

b) Se reseteará iptables a su estado original.

iptables -F borra todas las reglas de iptables, pero no las por defecto.

☒ c) La máquina ya no aceptará conexiones entrantes.

iptables -P INPUT DROP es una regla por defecto que dropea todas las conexiones entrantes. Enhorabuena, no puedes conectarte por ssh a tu máquina

d) La máquina aceptará todas las conexiones entrantes.

29) El protocolo Diffie-Hellman es empleado por SSH para...

a) Cifrar mediante un algoritmo asimétrico la comunicación cliente-servidor.

DH no cifra

b) Cifrar mediante un algoritmo simétrico la comunicación cliente-servidor.

☒ c) Intercambiar un secreto compartido o clave de sesión entre cliente y servidor. Si

d) SSH no emplea el protocolo Diffie-Hellman sino que usa RSA. Puede utilizar los 2 para diferentes propósitos

30) Usted crea una autoridad certificadora (AC) con el objetivo de emitir certificados digitales para varios servidores web de una organización. Con el objetivo de que el navegador de los usuarios no muestre ninguna alerta al conectarse por https a dichos servidores web...

☒ a) Los usuarios necesitarán importar en el navegador el certificado de la AC.

b) Los usuarios necesitarán importar en el navegador los certificados de todos los servidores web y el certificado de la AC.

No, con el de la AC llega, funciona con una cadena de confianza

c) Independientemente de los certificados que se importen, el navegador mostrará una alerta, al no ser la AC internacionalmente reconocida.

d) Los usuarios no necesitan importar nada. Es el servidor web el que debe importar el certificado de la AC.