Examen con respuestas con version ingles

Lexislación e Seguridade Informática (Universidade da Coruña)

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).

According to Community law, an information society service is

a) a service provided in exchange for remuneration (does not cover free services) and electronically
b) a service provided in exchange for remuneration, remotely, electronically and on a regular basis, at the individual request of the service recipient
c) a service normally provided in exchange for a remote remuneration, electronically and at the individual request of the service recipient
d) a service provided by electronic means, regardless of other characteristics (it can be paid or free, remotely or not, at individual request or multipoint point)

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.

in accordance with art 13 of the regulation of the organic law of protection of personal data

a) For the treatment of data of children under 18 years of age or more, the consent of the parents or legal representatives always requires
b) 16 years
c) 14 years

d) for the treatment of specially protected data of children under 16 years of age or older

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.

the national electronic identity document allows the electronic signature of documents with the consideration

a) Advanced electronic signature equivalent to the handwritten
b) from electronic signature to dry
c) of recognized electronic signature that is equivalent to the handwritten
d) electronic signature recognized when the judge recognizes it, thus being equivalent to the handwritten

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.

the consent on data protection

a) It is all manifestation of will, free, unequivocal, specific and informed, through which the interested party consents to the processing of personal data that concerns him. Consent cannot be silent
b) will always be required of the owner of the data, with the sole exception of the sources of access to the public, that is, those files whose query can be made by any person
c) It is all manifestation of will, free, unequivocal, specific and informed, through which the interested party consents to the processing of personal data that concerns him. Consent can be silent
d) is not valid when done by a child under 18 years. the consent of their parents or legal representatives is always required

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.

The European and Spanish community have opted for the same system to regulate electronic commercial communications, what is it?

a) the opt out system, which authorizes all electronic commercial communications, even without the prior consent of the recipient
b) the opt in system, which prohibits without exception the sending of electronic communications when they had not been requested or expressly authorized by the recipients with prior character
c) the opt out system, which authorizes all electronic commercial communications, even without the prior consent of the recipient, provided that the word advertising is recorded at the beginning of the message
d) the opt in system, which prohibits electronic commercial communications when they had not been requested or expressly authorized by the recipients on a prior basis, with the exception that there is a prior contractual relationship

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 referidas a la identidad étnica y de manera tácita para el resto de datos especialmente protegidos.

Data processing especially requires that the consent of the data owner be

a) granted expressly or tacitly
b) granted expressly
c) granted expressly and in the presence of a notary
d) expressly granted only for data referring to ethnic identity and tacitly for other specially protected data

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.

In accordance with Law 34/2002 of July 11 on services of the information society and electronic commerce, Where is an electronic contract entered into in which a consumer intervenes?

a) in the place agreed in the contract
b) at the place where the offer is made
c) at the place of establishment of the service provider
d) in the place of habitual residence of the consumer

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.

Spanish law requires a specific form for the validity of contracts?

a) yes. the contracts must be carried out in writing to be valid. Contracts carried out by electronic means are invalid, with the exception of those carried out by electronic signature
b) do not. the so-called spiritualist principle or freedom of form governs contracts. and in accordance with this principle the contracts concluded electronically are valid
c) yes. the contracts must be carried out in writing to be valid. Contracts carried out by electronic means are invalid in principle, unless a judge declares them valid
d) do not. the so-called spiritualist principle or freedom of form governs contracts. In addition, in many contracts the consent of the parties is not necessary to be valid

9) 21
   a) Raíz cuadrada de 484
   b) Ssh
   c) ftp
   d) telnet

21
   a) square root (pierwiastek kwadratowy) od 484 (22)
   b) ssh (22)
   c) ftp
   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.

in the context of computer security, the code
   a) refers to a known plugin for ettercap
   b) the code is an electronic verification code
   c) the code is a hash algorithm or summary
   d) the code uniquely identifies a vulnerability

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.
   d) Reflective attack que afecta a algunos servidores web.

   a) direct attack that affects all web servers
   b) reflective attack that affects all web servers
   c) direct attack that affects some web servers
   d) reflective attack that affects some web servers

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...)
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.

a) This file allows us to define multiple network configurations in order to connect our equipment in different networks. It is usually used in computers with mobility between home and work networks
b) This file allows us to configure where to look for certain types of administrative information (hosts, passwd)
c) This file is only located on those devices that have connectivity through switched-media networks, such as those from the practice laboratory, and is used for network packet management.
d) None of above

13) DMZ

a) Intranet.
b) Outranet.
c) Red perimetral.
d) Red Privada Virtual.

a) intranet
b) outranet
c) perimeter network (obwodowa)
d) virtual private network

14) Ataque LAND

a) Generación de paquetes con origen y destino la misma máquina, para que los auto-responda.
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.

a) generation of packages with origin and destination the same machine for the autoresponder
b) packet generation with origin of the machine to attack and destination of a broadcast address, to achieve a high amplification factor
c) packet generation with a broadcast address and destination the machine to attack
d) doesnt exists

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)
c) Debe coincidir con el nombre del sitio web (p. ej: www.udc.es)
d) Debe contener el nombre de la autoridad certificadora que emite dicho certificado.

in a digital certificate issued to a web server, the C field of the certificate
a) must contain the name and surname of the person in charge of the website
b) must contain a contact email address
c) must match the name of the website
d) must contain the name of the certifying authority that issues said certificate

16) OWASP TOP 10 del 2013 en tercera posición:
a) Password guessing.
b) Cross-Site Scripting.
c) DoS.
d) Buffer Overflow.

b)

17) NDP utiliza
a) Paquetes ARPv4
b) Paquetes ARPv6
c) Paquetes ICMPv4
d) Paquetes ICMPv6

d)

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.
c) Si no está vacío denota el uso de un proxy.
d) Se utiliza para hacer forwarding a nivel IP.

a) It has no relevance in the field of privacy and anonymity
b) It only includes the name or IP address of the web server
c) if it is not empty denotes the use of a proxy
d) It is used to forward IP level

19) Los TCP Wrappers
a) Filtran todos los servicios de red de nuestros sistemas.
b) Filtran todos los servicios TCP de nuestros sistemas.
c) Trabajan a nivel de kernel.
d) Ninguna de las anteriores es correcta.

a) filter all network services of our systems
b) filter all tcp services of our systems
c) they work at kernel level
d) none of above

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.
c) La 10.10.102.199 capturará 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.

considering as a reference the network of practices, in machine 100 arpon is configured statically. In 199 a mitm is made by arp spoofing of remote type between the 200 and the router. since 200 we navigate to different web pages
a) 199 captures the entire navigation package of 200 given that arpon detects arp spoofing but does not protect
b) 199 does not capture any web browsing traffic
c) 199 will capture a portion of the shipping package
d) 199 is blocked and a denial of service will occur due to the action of arpon

21) SHA3
a) Keccak
b) AES
c) X509
d) Sniffing

a)

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.

D

a) standard that defines a digital certificate format
b) standard to prevent DHCP spoofing
c) standard that allows multiple networks to share the same physical medium
d) standard for network access control

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.

a SYN packet to an open port will receive
b) SYN-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"
b) Nmap efectuará "port Scanning"
c) Nmap efectuará "host Discovery" y, si la máquina está "viva", efectuará "port scanning".
d) Nmap efectuará "fingerprinting".

A
fingerprinting: ping, nmap -O

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.

the anonymity provided by the Tor network is based on

a) use end-to-end encryption (from the user's machine to the destination machine)
b) use a network parallel to the internet, with its own infrastructure
c) hide the identity of intermediate nodes
d) none of above

26) *Un ataque de tipo CAM flooding...*

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.
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.

a flood type CAM attack

a) It is based on filling the CAM table of the switch, so that it behaves like a hub
b) it will not work if users have configured static ARP mapping on their computers
c) in a mitm attack
d) It is based on associating the MAC address of the attacker with the IP address of the switch and thus receiving all the traffic that stops by the switch

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.
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.

a) they are a protection against DoS that consists of using an independent data structure parallel to the Transmission Control Block to avoid overloading the latter
b) they are a protection against DoS that is based on using the TCP sequence number to encode data and thus reset connection space only when the final confirmation message is received
c) they are a protection against the capture of SSL sessions through the use of cookies in a mitm attack
d) they are a protection against DoS that consists of storing in a cookie customer identification data, to know what is generating the attack

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.
c) La máquina ya no aceptará conexiones entrantes.
d) La máquina aceptará todas las conexiones entrantes.

on your lab machine from a console with root permissions you run, what will happen then?

a) all INPUT rules will be deleted and rules will be listed on screen
b) iptables will be reset to its original state
c) the machine will no longer accept incoming connections
d) The machine will accept all incoming connections

29) El protocolo Diffie-Hellman es empleado por SSH para...
a) Cifrar mediante un algoritmo asimétrico la comunicación cliente-servidor.
b) Cifrar mediante un algoritmo simétrico la comunicación cliente-servidor.
c) Intercambiar un secreto compartido o clave de sesión entre cliente y servidor.
d) SSH no emplea el protocolo Diffie-Hellman sino que usa RSA.

the protocol is used by ssh to

a) encrypt client-server communication using an asymmetric algorithm
b) encrypt client-server communication using a symmetric algorithm
c) exchange a shared secret or session key between client and server
d) ssh does not use the protocol but uses RSA

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.
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.

You create a certificate authority with the aim of issuing digital certificates for several web servers in an organization. in order that the user's browser does not show any alert when connecting via https to these web servers

a) Users will need to import the CA certificate into the browser
b) Users will need to import in the browser the certificates of all web servers and the CA certificate
c) Regardless of the certificates that are imported, the browser will display an alert, as it is not the internationally recognized CA
d) Users do not need to import anything. It is the web server that should import the certificate from the CA.

2016

1.- 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.

a)

2.- De acuerdo con la Directiva de la Comunidad Europea el prestador de servicios de hospedaje en internet (hosting) estará exento de responsabilidad por los contenidos de los usuarios de sus servicios cuando:

a) actúe como mero intermediario de contenidos ajenos y no tenga conocimiento efectivo de la ilicitud de la actividad o de la información que alberga. Y, en caso de tener conocimiento efectivo, deberá actuar con prontitud para retirar los datos o para hacer que el acceso a los mismos sea imposible.
b) no sea el creador de los contenidos que hospeda, ni haya tenido la iniciativa de hospedarlos, con independencia de que tenga o no conocimiento efectivo de la ilicitud de los mismos.
c) albergando contenido ilícito, la pérdida de los titulares de los derechos por dicho contenido no sea superior a medio millón de euros.
d) así lo declare un juez, pues se presume siempre la responsabilidad del ISP que realiza servicios de hosting porque se trata de un intermediario imprescindible par la comisión de cualquier ilícito.

in accordance with the directive of the European community the provider of hosting and internet services (hosting) will be exempt from responsibility for the contents of the users of their services when

a) when it acts as a mere intermediary of old content and does not have effective knowledge of the illegality of the activity or of the information it houses and, in case of having effective knowledge, it must act promptly to withdraw the data or to make access to themselves be impossible
b) when he is not the creator of the content he hosts, nor has he had the initiative to host them, regardless of whether or not he has effective knowledge of their illegality
c) when harboring illicit content, the loss of rights holders for such content does not exceed half a million euros
d) when a judge so declares, because the responsibility of the ISP that performs hosting services is always presumed because it is an essential intermediary by the commission of any illicit

3.- ¿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 contrato llevados a cabo por medios electrónicos son inválidos, con la excepción de aquell 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.

b)

4.- 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).

c)

5.- Escoja la opción correcta:

a) Los servicios de intermediación (ISP) deben colaborar con la autoridad judicial cuando ésta les ordena la interrupción de un servicio, la retirada de contenidos o la imposibilidad de acceder a determinados datos. Esta obligación surge únicamente cuando se ha vulnerado la propiedad intelectual o industrial.

b) El deber de colaboración de los servicios de intermediación (ISP) con las autoridades, no es exigible cuando al ISP se le aplica alguna de las exenciones de responsabilidad.

c) El incumplimiento del deber de colaboración supone la pérdida de las exenciones de responsabilidad en el plazo de dos días naturales desde que el ISP recibe la orden de colaboración.

d) Los servicios de intermediación (ISP) deben colaborar con la autoridad judicial cuando ésta les ordene la interrupción de un servicio, la retirada de contenidos o la imposibilidad de acceder a determinados datos.

a) Brokerage services must collaborate with the judicial authority when they are ordered to interrupt a service, withdraw content or the inability to access remote data. This obligation arises only when intellectual or industrial property has been violated
b) The duty of collaboration of the intermediation services with the authorities is not enforceable when the ISP applies any of the disclaimers
c) the breach of the duty of collaboration implies the loss of the disclaimers within two calendar days after the ISP receives the order of collaboration
d) intermediation services must collaborate with the judicial authority when it is ordered by the interruption of a service, the withdrawal of content or the inability to access certain data

6.- ¿En qué consiste la responsabilidad extracontractual?

a) Se deriva de una acción u omisión que causa un daño a otro, interviniendo culpa o negligencia, que obliga a reparar el daño causado. Entre el causante del daño y el que lo sufre no media contrato alguno. No es aplicable a los ISP.

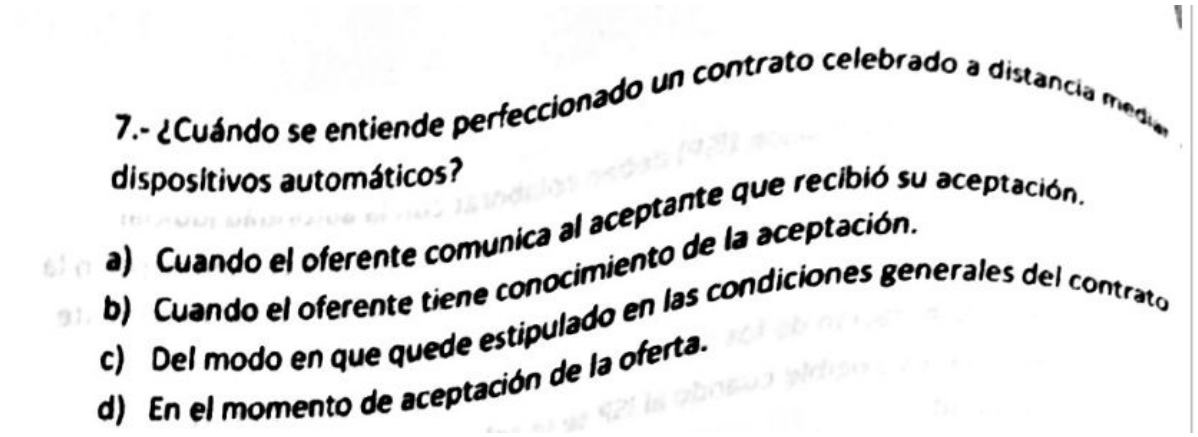
b) Forma parte del régimen general de responsabilidad civil junto con la responsabilidad contractual, por lo que se aplica también al ámbito informático. En el caso de los servicios de intermediación (ISP) se aplica al intermediario siempre que éste no haya perdido las exenciones.

c) Es la derivada de una acción u omisión que causa daño a otro, interviniendo culpa o negligencia, que obliga a reparar el daño causado. Entre el causante del daño y el que lo sufre no media contrato alguno.

d) Es la responsabilidad que obliga a reparar el daño causado cuando se causa daño a otro. Es aplicable al ámbito civil en general y al ámbito electrónico sólo en los casos previstos por el art. 17 de la ley de servicios de la sociedad de la información y de comercio electrónico.

what is the non-contractual liability

a) it is derived from an action or omission that causes damage to another, intervening fault or negligence, which forces to repair the damage caused. between the cause of the damage and the one who suffers it there is no half contract. not applicable to ISPs
b) It is part of the general civil responsibility regime along with contractual responsibility, so it also applies to the information field. in the case of intermediation services, it is applied to the intermediary provided that he has not lost the exemptions
c) it is the derivative of an action or omission that causes damage to another, intervening fault or negligence, which forces to repair the damage caused. between the cause of the damage and the one who suffers it there is no half contract.
d) It is the responsibility that forces to repair the damage caused when damage is caused to another. It is applicable to the civil field in general and to the electronic field only in the cases provided for in article 17 of the law of services of the information society and electronic commerce


7.- ¿Cuándo se entiende perfeccionado un contrato celebrado a distancia mediante dispositivos automáticos?

a) Cuando el oferente comunica al aceptante que recibió su aceptación.
b) Cuando el oferente tiene conocimiento de la aceptación.
c) Del modo en que quede estipulado en las condiciones generales del contrato
d) En el momento de aceptación de la oferta.

when it is understood perfected a contract concluded at medium distance automatic devices
a) when the offeror informs the acceptor that he received his acceptance
b) when the offeror is aware of the acceptance
c) in the manner stipulated in the general conditions of the contract
d) at the time of acceptance of the offer

8.- ¿La oferta electrónica es una declaración de voluntad del oferente para la celebración de un contrato?

a) **No. La oferta electrónica no es una declaración de voluntad para la celebración un contrato.**
b) **Sí. La oferta electrónica o publicidad electrónica es una declaración de voluntad para la celebración de un contrato.**
c) **Sí.**
d) **No. La oferta electrónica no es una declaración de voluntad. La declaración de voluntad requiere que el oferente ratifique su deseo de celebrar el contrato cuando el aceptante ha aceptado llevarlo a cabo.**

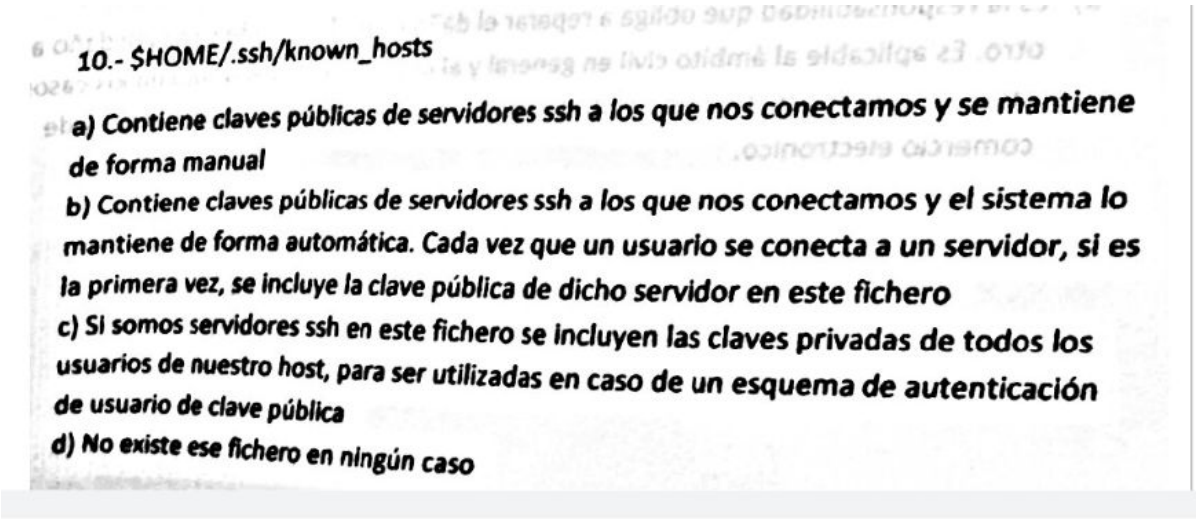
Is the electronic offer a declaration of will of the bidder for the conclusion of a contract?

a) do not. The electronic offer is not a declaration of will for the conclusion of a contract
b) yes. the electronic offer or electronic advertising in a declaration of will for the conclusion of a contract
c) yes
d) do not. The electronic offer is not a declaration of will. The declaration of will requires the bidder to ratify their desire to conclude the contract when the acceptor has agreed to carry it out

9.- En SSL, ¿qué protocolo se encarga del intercambio de mensajes sobre avisos y errores?

a) HP
b) RP
c) AP
d) CCSP

c)



10.- $HOME/.ssh/known_hosts

a) Contiene claves públicas de servidores ssh a los que nos conectamos y se mantiene de forma manual

b) Contiene claves públicas de servidores ssh a los que nos conectamos y el sistema lo mantiene de forma automática. Cada vez que un usuario se conecta a un servidor, si es la primera vez, se incluye la clave pública de dicho servidor en este fichero

c) Si somos servidores ssh en este fichero se incluyen las claves privadas de todos los usuarios de nuestro host, para ser utilizadas en caso de un esquema de autenticación de usuario de clave pública

d) No existe ese fichero en ningún caso

a) Contains public keys of ssh servers to which we connect and is maintained manually
b) contains public keys of ssh servers to which we connect and the system maintains it automatically. Each time a user connects to a server, if it is the first time, the public key of that server is included in this file
c) if we are ssh servers in this file the private keys of all the users of our host are included, to be used in case of a public key user authentication scheme
d) there is no file in any case

11.- PKCS

a) Es otra forma de denominar al X509
b) Protocolo de intercambio de claves de sesión para SSL que forma parte del Change Cipher Spec Protocol
c) Grupo de estándares de criptografía de clave pública
d) Ninguna de las anteriores es correcta

a) is another way to name the X509
b) session key exchange protocol for SSL that is part of the Change Cipher Spec Protocol
c) group of public key cryptography standards
d) none of the above is correct

12.- Un fichero .pem

a) Puede contener una clave pública, clave privada y certificado raíz
b) Es un contenedor de certificados digitales por lo que únicamente puede contener claves públicas, las privadas siempre irán en los ficheros .key
c) Es un formato únicamente reservado para contener listas de revocación de certificados
d) Ninguna de las anteriores es correcta

a) may contain a public key, private key and root certificate
b) it is a container of digital certificates so it can only contain public keys, the private ones will always go in the .key files

c) is a format only reserved for containing certificate revocation lists
d) none of the above

13.- Relacione la siguiente cadena
$6$9xLcXzqY$fa4.hFYGFgTioVKL25mWZvO5ck3XF0E7jKYlAPAcvHRzwlMZUsDJzyodFa/9vXZ69fJ
thxwo3twyUQ3K/XRbw1

a) certificado para https X509
b) clave privada de host en ssh
c) shadow
d) secuencia de caracteres al azar sin relación con tema alguno

Relate the following string
a) certificate for https X509
b) private host key in ssh
c) shadow
d) random character sequence without relation to any subject

14.- Un certificado digital

a) Está firmado utilizando la clave privada del propietario de la clave pública de dicho certificado
b) Está firmado utilizando la clave privada de la correspondiente autoridad certificadora
c) Está firmado utilizando la clave privada del emisor de una comunicación segura que utiliza la clave pública de dicho certificado
d) Ninguna de las anteriores

A digital certificate
a) is signed using the private key of the owner of the public key of said certificate
b) is signed using the private key of the corresponding certifying authority
c) is signed using the private key of the issuer of a secure communication using the public key of said certificate
d) none of the above

15.- La generación es un ataque contra la ...

a) disponibilidad
b) confidencialidad
c) autenticidad
d) integridad

Generation is an attack against
a) availability
b) confidentiality
c) authenticity
d) integrity

16.- RC4

a) cifrador de bloque
b) cifrador de flujo
c) cifrador de clave pública y privada
d) cifrador de patatas

a) block cipher
b) flow cipher
c) public and private key encryption
d) potato cipher

17.- La dirección ::1

a) reloj interno en NTP
b) localhost
c) multicast de todas las direcciones link-local del segmento
d) no existe esa dirección

The address ::1
a) internal clock in NTP
b) localhost
c) multicast of all link-local segment addresses
d) that address does not exist

18.- shodan

a) motor de búsqueda de equipos y dispositivos específicos
b) analizador de vulnerabilidades web
c) herramienta de esteganografía
d) analizador de configuraciones de cortafuegos

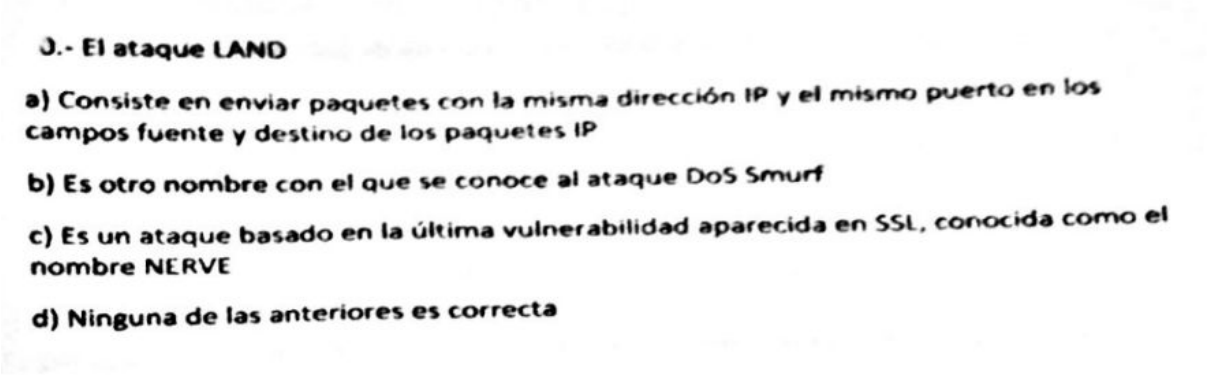
a) search engine for specific equipment and devices
b) web vulnerability analyzer
c) steganography tool
d) firewall configuration analyzer

19.- .onion

a) plataforma interactiva para el manejo de proxys de tipo transparente abiertos en la red
b) dominio recientemente aprobado por la ICANN que aglutina la totalidad de máquinas que acceden a la red tor
c) pseudo dominio de nivel superior genérico que indica una dirección IP anónima accesible mediante la red tor
d) no es un dominio o pseudodominio. Es el fichero de configuración de todo equipo que accede a la red tor, que mantiene el conjunto de nodos tor a utilizar en las comunicaciones en cada momento

a) interactive platform for handling transparent open network proxies

b) domain recently approved by ICANN that brings together all the machines that access the tor network
c) pseudo generic top-level domain indicating an anonymous IP address accessible through the tor network
d) it is not domain or pseudo-domain. The configuration file of all equipment that accesses the tor network, which maintains the set of tor nodes to be used in communications at all times



J.- El ataque LAND

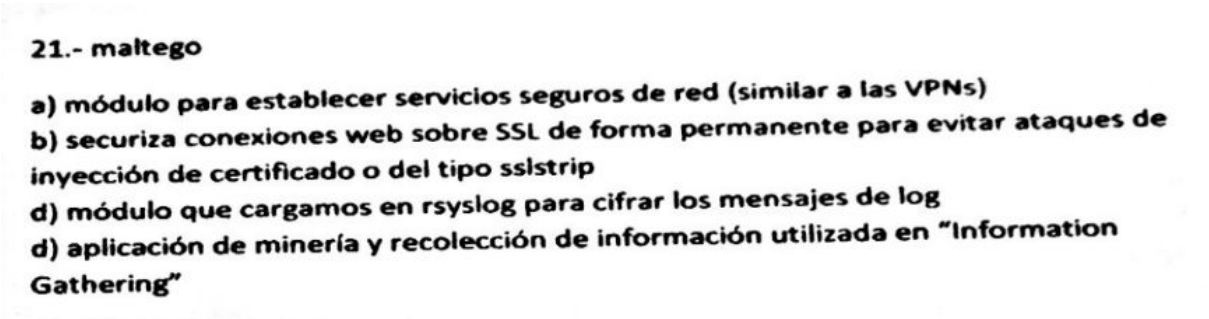
a) Consiste en enviar paquetes con la misma dirección IP y el mismo puerto en los campos fuente y destino de los paquetes IP

b) Es otro nombre con el que se conoce al ataque DoS Smurf

c) Es un ataque basado en la última vulnerabilidad aparecida en SSL, conocida como el nombre NERVE

d) Ninguna de las anteriores es correcta

a) consists of sending packets with the same IP address and the same port in the source and destination fields of the IP packets (only IP, open port)
b) is another name by which the DoS Smurf attack is known
c) is an attack based on the last vulnerability appeared in SSL, known as the name NERVE
d) none of the above is correct



21.- maltego

a) módulo para establecer servicios seguros de red (similar a las VPNs)
b) securiza conexiones web sobre SSL de forma permanente para evitar ataques de inyección de certificado o del tipo sslstrip
d) módulo que cargamos en rsyslog para cifrar los mensajes de log
d) aplicación de minería y recolección de información utilizada en "Information Gathering"

a) module to establish secure network services (similar to VPNs)
b) secure web connections over SSL permanently to avoid certificate injection attacks or sslstrip type
c) module that we load in rsyslog to encrypt log messages
d) application of mining and information collection used in "Information Gathering"

22.- Usted abre una conexión ssh contra su máquina de laboratorio en la 10.10.102.XX y le solicita el correspondiente login o nombre de usuario y password.

a) En el correspondiente proceso de autenticación se utiliza el algoritmo criptográfico MD5
b) En el correspondiente proceso de autenticación se utiliza el algoritmo criptográfico SHA2
c) En el correspondiente proceso de autenticación se utiliza kerberos
d) Ninguna de las anteriores es correcta

You open a ssh connection against your laboratory machine at 10.10.102.XX and ask for the corresponding login or username and password
a) the cryptographic algorithm MD5 is used in the corresponding authentication process
b) the SHA2 cryptographic algorithm is used in the corresponding authentication process
c) in the corresponding authentication process kerberos is used
d) none of the above is correct

23.- Usted tiene instalada una aplicación en su PC y se acaba de publicar un Zero-day sobre la misma. ¿Qué debe hacer?

a) Ir al sitio Web del fabricante de la aplicación y descargar el parche que soluciona el Zero-day
b) Informarse sobre la vulnerabilidad en cuestión
c) Nada. Al ser un Zero-day, no hay nada que hacer
d) Configurar el firewall, de modo que no sea posible explotar el Zero-day

You have an application installed on your PC and a Zero-day has just been published on it. What should he do?
a) go to the website of the manufacturer of the application and download the patch that solves the Zero-day
b) find out about the vulnerability in question
c) nothing. Being a Zero-day, there is nothing to do
d) configure the firewall, so that it is not possible to exploit the Zero-day

24.- En su máquina virtual (10.10.102.XX), en el entorno de prácticas del laboratorio, ejecuta, como usuario privilegiado el siguiente comando:

nmap 10.10.102.27

Indique la respuesta correcta:

a) nmap efectuará sólo "host discovery"
b) nmap efectuará sólo "port scanning"
c) nmap efectuará "host discovery" y, si la máquina está "viva", efectuará "port scanning"
d) nmap efectuará "host discovery", "port scanning" y "fingerprinting"

C
host discovery -sP

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

a) ocultar la dirección IP real del usuario
b) cifrar el tráfico desde la máquina del usuario hasta la máquina de destino
c) usar una infraestructura de red paralela a Internet
d) usar proxies residentes en países sin regulación sobre Internet

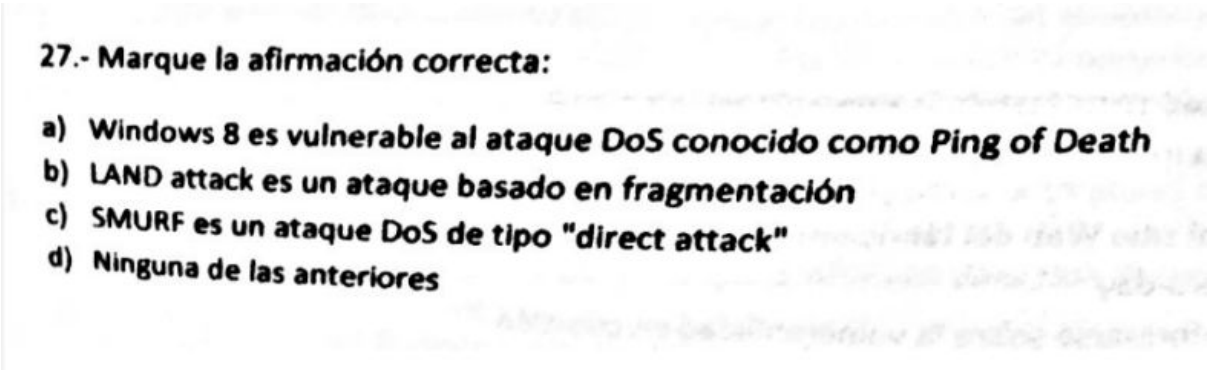
The anonymity provided by the Tor network is based on
a) hide the user's real IP address
b) encrypt the traffic from the user's machine to the destination machine
c) use a network infrastructure parallel to the internet
d) use proxies residing in countries without internet regulation

26.- Un ataque de tipo CAM flooding...

a) No funcionará si los usuarios han configurado mapeado ARP estático en sus equipos
b) También se conoce como ARP spoofing o ARP poisoning
c) 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
d) Ninguna de las anteriores

A flood type CAM attack
a) It will not work if users have configured static ARP mapping on their computers
b) ARP spoofing or ARP poisoning is also known

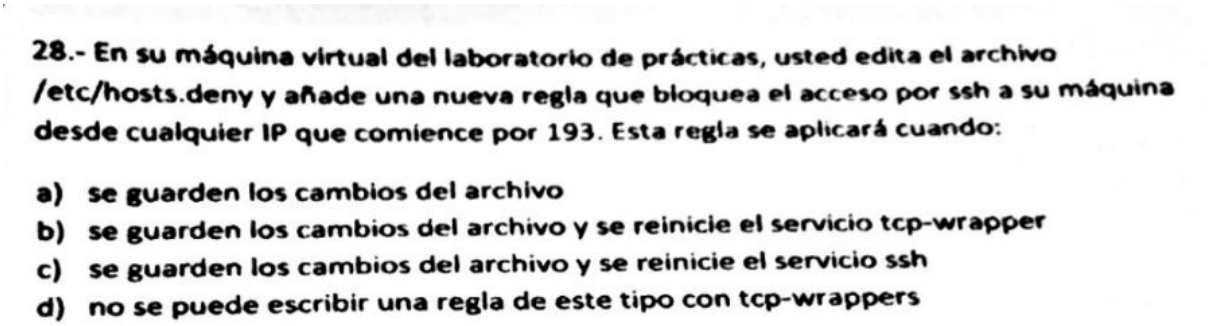
c) is based on associating the MAC address of the attacker with the IP address of the switch and thus receiving all the traffic that passes through the switch
d) none of the above



27.- Marque la afirmación correcta:

a) Windows 8 es vulnerable al ataque DoS conocido como Ping of Death
b) LAND attack es un ataque basado en fragmentación
c) SMURF es un ataque DoS de tipo "direct attack"
d) Ninguna de las anteriores

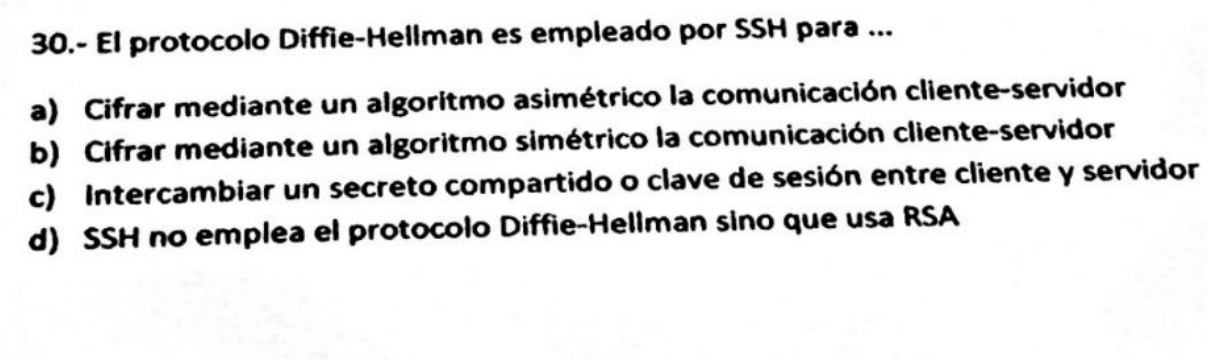
Mark the correct statement
a) Windows 8 is vulnerable to the DoS attack known as Ping of Death
b) LAND attack is a fragmentation based attack
c) SMURF is a DoS attack of type "direct attack"
d) none of the above



28.- En su máquina virtual del laboratorio de prácticas, usted edita el archivo /etc/hosts.deny y añade una nueva regla que bloquea el acceso por ssh a su máquina desde cualquier IP que comience por 193. Esta regla se aplicará cuando:

a) se guarden los cambios del archivo
b) se guarden los cambios del archivo y se reinicie el servicio tcp-wrapper
c) se guarden los cambios del archivo y se reinicie el servicio ssh
d) no se puede escribir una regla de este tipo con tcp-wrappers

A



30.- El protocolo Diffie-Hellman es empleado por SSH para ...

a) Cifrar mediante un algoritmo asimétrico la comunicación cliente-servidor
b) Cifrar mediante un algoritmo simétrico la comunicación cliente-servidor
c) Intercambiar un secreto compartido o clave de sesión entre cliente y servidor
d) SSH no emplea el protocolo Diffie-Hellman sino que usa RSA

The Diffie-Hellman protocol is used by SSH to ...
a) encrypting client-server communication using an asymmetric algorithm

b) client-server communication encryption using a symmetrical algorithm
c) exchange of a shared secret key or session key between the client and server
d) SSH does not use the Diffie-Hellman protocol, but uses RSA

LSI examen enero 2013/2014

1. LAG:
a) Linux Access Grant
b) Link Aggregation Channel
c) ..
d) ..

2. Buffer Overflow:
a) Modificación
b) Interrupción
c) Generación
d) ..

3. Idle Scan:
a) Relacionado con Ip Spoofing, IP ID, control de estado entre otros.
b) No relacionado con Ip Spoofing pero sí con IP ID
c) La a) es correcta pero sin Ip Spoofing
d) Ninguna de las anteriores

4. Top 10 OWASP 2013:
a) Cross-Site Scripting (XSS)
b) Network Sniffing
c) Injection
d) Broken Session Control Management

5. AES:
a) Cifrado Simétrico
b) Cifrado Asimétrico
c) Función Hash
d) Función de codificación

6. modsecurity:
a) ..
b) ..
c) Mod de Apache para evitar DDoS
d) Firewall de aplicación web

7. mangle en iptables:
a) ..
b) NAT
c) Modificación de paquetes
d) ..

8. proxy transparente:
a) Eres totalmente anonimo
b) Totalmente desaconsejable si quieres ganar anonimicidad.
c) ..
d) ..

9. La ip de ntp 127.127.1.1 significa:
a) Nivel superior
b) Nivel inferior
c) El reloj interno de la máquina
d) Ninguna de las anterioes

10. En los tipos de backups:
a) ..
b) El diferencial es más rápido que el incremental haciendo el backup.
c) El diferencial es más sencillo que el incremental restaurando.
d) Todas las anteriores son ciertas

11. Diferencia entre tcp-wrappers e iptables:
a) ..
b) Los tcp-wrappers se aplican antes que las reglas de iptables.
c) Los tcp-wrappers se aplican a nivel de sistema operativo y los iptables a nivel de aplicación.
d) Ninguna de las anterioes.

12. En cifrado asimétrico se cifra:
a) Con la clave pública del receptor
b) Con la clave privada del emisor
c) Con la clave pública del emisor
d) Con la clave privada del receptor

13. La función:
a) Sha3 es usada en los protocolos de seguridad actuales.
b) Kekkan..? es el algoritmo que implementa Sha2
c) ..
d) Ninguna de las anteriores

14. X509:
a) PKI
b) ..
c) ..
d) Estandar de sensores de red

15. CVE-2003-5007:
a) Clave de identificación única para vulnerabilidades.
b) "" de categorías.
c) ..
d) ..

16. Port-knocking:
a) Un mecanismo para tirar host, coloquialmente hablando "knockear"
b) Con esto ves a través de la cámara de tu profesor de LSI
c) ..
d) Técnica empleada para abrir servicios/puertos enviando una secuencia de paquetes a puertos determinados

17. La manera más eficiente de comprobar si una máquina esta up:
a) ICMP Echo Request (Ping)
b) TCP SYN ← Creo
c) TCP ACK
d) ARP Request

18. CAM Flooding:
a) Rebentar el CAM del switch objetivo con el objetivo de que actúe como un Hub
b) No funciona utilizando ARP estático
c) Es lo mismo que ARP Spoofing/Poisoning
d) ..

19. En las redes Tipo TOR:
a) Es infalible
b) Hay tres tipos de entidades: Onion Router, Onion Proxy, y Anonymizers
c) Es necesario un entry node, middle node, y exit node
d) El exit node va siempre cifrado a su destino.

20. El Reflective SYN FLOOD
a) Empledo de botnets.
b) ..
c) Se le manda a la víctima un paquete con la dirección ip de origen su dirección de destino para que entre en un bucle infinito.
d) Utiliza nodos intermedios para repetir.. (broadcast)

21. El Common Name de un certificado digital es:
a) El nombre y apellidos
b) Un correo electrónico
c) El nombre de dominio
d) El nombre de la CA

Protección y Seguridad de la Información (junio 2009)

1.- DVL
a) Distribución GNU/Linux que aglutina las principales herramientas en ataque orientada a la realización de auditorías de seguridad
b) **Distribución GNU/Linux repleta de inseguridades orientada al aprendizaje**
c) Distribución GNI/Linux que incluye los desarrollos LVS orientada a Alta Disponibilidad
d) Ninguna de las anteriores

2.- La herramienta Xprobe está orientada a
a) Backups en modo cliente-servidor
b) Detección de sniffers en un segmento de red
c) Cifrar sesiones de trabajo que no soporten SSL
d) **Identificación remota de sistemas operativos basada en ICMP**

3.- Un amigo está haciendo referencia al nmap y te habla de un idle scan
a) Hace referencia a la decodificación de firmas para identificar el sistema operativo de un sistema remoto de forma pasiva
b) Hace referencia a un escaneo de puertos
c) Hace referencia a un escaneo suplantando otras IPs
d) Hace referencia a un escaneo mediante retardos

4.- Si enviamos un paquete FIN a un sistema generalmente nos responderá
a) FIN ante un puerto cerrado y nada si está abierto
b) RST|ACK ante un puerto abierto y nada si está cerrado
c) RST|ACK ante un puerto cerrado y nada si está abierto
d) Ninguna de las anteriores

5.- El proceso de firma digital
a) Cifra la huella con la clave pública del emisor
b) Cifra la huella con la clave pública del receptor
c) Cifra la huella con la clave privada del emisor
d) Ninguna de las anteriores es correcta

6.- Si ejecutamos el comando # ac
a) Total de tiempo de cpu utilizado por los procesos de un usuario, en este caso del root
b) Información de fecha, hora, etc., de las sesiones abiertas por un usuario, en este caso del root
c) Relación de comandos ejecutados en el proceso de accounting, en este caso del root
d) Total de horas de conexión de un usuario, en este caso del root

7.- zabbix
a) Herramienta de monitorización distribuida
b) Herramienta para backups distribuidos
c) Herramienta de detección de interfaces en modo promisc
d) Ninguna de las anteriores

8.- ISO27002
a) Guía de buenas prácticas en seguridad
b) Estándar que se centra en la gestión de la seguridad de la información (análisis de riesgos, planes de contingencia, etc.)
c) Guía de fases para "securizar" redes WIFI
d) Estándar que define configuraciones seguras de plataformas de "backups"

9.- En una red de tomas de tierra, ¿qué es el TGB?
a) Barra principal
b) Barras secundarias
c) Backbone de la red de tomas de tierra
d) Ninguna de las anteriores

11.- LTO4
a) 400MB nativos
b) 200GB nativos
c) 400GB nativos
d) 800GB nativos

13.- ¿Qué entorno de trabajo es el característico del software Tivoli?
a) Sniffers
b) Gestión de almacenamiento y backups
c) DDoS
d) Filtrado por tcpwrappers

14.- ¿Qué método de sniffing hace spoofing sobre los switches pensando en un entorno de medio conmutado?
a) MAC Flooding
b) ARP Spoofing
c) MAC Trusted
d) MAC Duplicating

15.- Puerto 514
a) ntp
b) X509 – Autoridades Certificadoras
c) syslog
d) Ninguno anteriores

16.- Atendiendo al nivel de importancia de los mensajes de log, ¿qué afirmación es correcta?
a) EMERG menor importancia que CRIT
b) ALERT menor importancia que CRIT
c) CRIT menor importancia que CRIT
d) Ninguna de las anteriores

17.- Direcciones IPV6
a) 32
b) 64
c) 128
d) 256

18.- /etc/nsswitch.conf
a) Esquema de fuentes para hosts, dns, autenticación, etc.
b) Esquema de resolución del sistema y el dominio.
c) Configuración de correspondencia entre máquinas y direcciones Ethernet
d) Ninguna de las anteriores

19.- Port Security en CISCO
a) enable switchport port-security
b) port-security on
c) switchport port-security
d) port-security activate de una … vez

20.- AES
a) clásico
b) flujo
c) bloque
d) asimétrico

Junio 2001

1.- La modificación es una categoría de ataque contra
a)Confidencialidad
b)Disponibilidad
c)Integridad
d)Austeridad

2.- Un ataque por repetición es de tipo
a)activo
b)pasivo
c)inverso
d)mixto

3.- Que tecnica de "scanning de puertos" se conoce como escaneo de "media apertura"
a)TCP SYN Scaning
b)TCP connect() scaning
c)TCP open() scaning
d)TCP reserve ident scaning