Preguntas examen

Lexislación e Seguridade Informática (Universidade da Coruña)

LEGISLACIÓN Y SEGURIDAD INFORMÁTICA 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

2. De acuerdo con la Directiva de la Comunidad Europea el prestador de servicios de hospedaje en internet 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 licitud de la actividad o de la información que alberga. Y, en caso de tener conocimiento efectivo, deberá actuar con prontitud para retirar los datos para hacer que el acceso a los mismo 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 mismo.
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 para la comisión de cualquier ilícito.

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 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. Año. 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.

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, u 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 independencias de otras características (puede ser remunerado o gratuito, a distancia o no, petición individual o punto-multipunto)

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 una 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 esta les ordene la interrupción de un servicio, la retirada de contenidos o la imposibilidad de acceder a determinados datos.

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 este 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 solo en los casos previstos por el art. 17 de la ley de servicio de la sociedad de la información y de comercio electrónico.

7. ¿Cuando 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.

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 de un contrato.
b. Año. 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 desea de celebrar el contrato cuando el aceptante ha aceptado llevarlo a cabo.

9. En SSL, ¿qué protocolo se encarga del intercambio de mensajes sobre avisos y errores?
a. HP
b. RP
c. AP
d. CCSP

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.

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.

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 irán siempre en los ficheros .key
c. Es un formato únicamente reservado para contener listas de renovación de certificados.
d. Ninguna de las anteriores es correcta.

13. Relacione la siguiente cadena $6$9balñgbñafk.gaibofalanfñafwfbaif/lk.angbagbvÑF/blñagbagñvb
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.

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.

15. La generación es un ataque contra la…
a. disponibilidad.
b. confidencialidad.
c. autenticidad.
d. integridad.

16. RC4
a. cifrador de bloque.
b. cifrador de flujo.
c. cifrador de clave pública y privada.
d. cifrador de patatas.

17. La dirección ::1
a. reloj interno de ntp.
b. localhost.
c. multicast de todas las direcciones link-local del segmento.
d. no existe esa dirección.

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.

19. .onion
a. plataforma interactiva para el manejo de proxys de todo 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 pseudo dominio. 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.

20. El ataque LAND.
a. Consiste en enviar paquetes con la misma dirección IP y el mismo puertos 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 de NERVE.
d. Ninguna de las anteriores.

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.
c. módulo que cargamos en rsyslog para cifrar los mensajes del log.
d. aplicación de minería y recolección de información utilizada en “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.

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 Zero-day, no hay nada que hacer.
d. Configurar el firewall, de modo que no sea posible explotar el Zero-day.

24. En su máquina virtual (10.10.102.XX), en el entorno de prácticas de laboratorio, ejecuta, como usuario privilegiado el siguiente comando: nmap 10.10.102.27:
a. nmap efectuará solo host discovery.
b. nmap efectuará solo 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.

25. El anonimato en 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.

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

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 una ataque DoS de tipo “direct attack”.
d. Ninguna de las anteriores

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.

29. WPA2:
a. AES
b. DES
c. 3DES
d. RC4

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 empleó el protocolo Diffie-Hellman sino que usa RSA

Otros examenes:

1. SYN-COOKIES
a. Son una protección contra Dos que consiste en emplear una estructura de datos independiente y paralela a la transmisión 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 Ddos que consiste en almacenar en una cookie datos identificativos de los clientes, para saber quien está generando el ataque

2. En su máquina de laboratorio, desde una consola, con permiso root, usted ejecuta: #iptables -P INPUT DROP; iptables -F ¿qué sucederá entonces?
a. Se borrarán todas las reglas de INPUT y se listaran las reglas por pantalla.
b. Se reseteara iptables a su estado original.
c. La máquina ya no acepta conexiones entrantes.
d. La máquina acepta todas las conexiones entrantes.

3. 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.

4. 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 muestro 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 importan, el navegador mostrará una alerta, al no ser la AC internacionalmente reconocida.
d. Los usuarios no necesitan importar nada. En el servidor web el que debe importar certificado de la AC.

5. 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.
c. Debe coincidir con el nombre del sitio web.
d. Debe contener el nombre de la autoridad certificadora que emite dicho certificado.

6. OWASP TOP 10 del 2013 en tercera posición:
a. Password guessing
b. Cross-site Scripting
c. Dos
d. Buffer Overflow

7. NDP utiliza
a. Paquetes ARPv4
b. Paquetes ARPv6
c. Paquetes iCMPv4
d. Paquetes ICMPv6

8. 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 de ip.

9. 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

10. Considerando como referencia la red de prácticas, en la maquina 10.10.102.200 se configura arpon de forma estática. En la 10.10.10.102.199 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 paginas web.
a. La 10.10.102.199 captura la totalidad de la paqueteria de navegacion de la 10.10.102.200 dado que arpon detecta el ARP spooging pero no protege.
b. La 10.10.102.199 no captura ningun trafico de la navegacion.
c. La 10.10.102.199 capturarara una parte de la paqueteria de la navegación.
d. La 10.10.102.199 quedara bloqueada y se le producira una denegación de servicio por la acción de arpon.

11. SHA3
a. Keccak
b. AES
c. X809
d. Sniffing

12. 802.1.x
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.

13. Un paquete SYN a un puerto recibirá
a. Un SYN
b. Un SYN-ACK
c. Un ACK
d. Ninguna de las anteriores

14. Desde su máquina virtual (10.10.102.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 tal la máquina está viva, efectuará “port scanning”
d. Nmap efectuará “fingerprinting”

15. El anonimato que proporciona la red Tor se basa en…
a. Usar cifrado extremo-extremo (desde la máquina del usuario hasta la máquina destino)
b. usar una red paralela a internet, con infraestructura propia.
c. Ocultar la identidad de los nodos intermedios.
d. Ninguna de las anteriores.

16. Un ataque de tipo CAM flooding…
a. Se basa en llenar la tabla CAM del switch, para que este 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.

17. La Comunidad europea y españa han optado por un mismo sistema para regular las comunicaciones comerciales electrónicas, ¿Cual es?

a. El sistema opt out, que autoriza todas las comunicaciones comerciales electrónicas, aun 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, aun sin consentimiento previo del destinatario, siempre que conste la palabras “publicidad” al contenido 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.

18. 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.

19. De acuerdo la ley 34/2002, de 11 de julio de servicios de la sociedad de la información y el comercio electrónico ¿donde se entiende un contrato electrónico en que interviene un consumidor (BC2)?

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

20. ¿El derecho español exige una forma concreta de 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 llevado 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 que sean válidos.

21. Según el derecho comunitario a un servicio de la sociedad de la información es..
a. Un servicio prestado a cambio de remuneración 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.

22. 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 datos de menores de 16 o más, se precisa siempre el consentimiento de los padres o representantes legales.
c. Para el tratamiento de datos de menores de 14 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.

23. 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.

24. El consentimiento en materia de protección de datos…

a. Es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado considera el tratamiento de datos personales que le conciernen. El consentimiento no pudo ser tácito.
b. Se exigirá siempre el titular de los datos, con la única excepción de las fuentes de acceso pública (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 padre o representaciones legales.

25. 21
a. Raíz cuadrada de 484.
b. SSH
c. FTP
d. TELNET

26. En el contrato de la seguridad informática, el código CVE-2014-0160…
a. Se refiere a un conocido plugin para ettercap
b. Es un codigo de verificacion electronica.
c. Es un algoritmo de hash o resumen.
d. Identifica unívocamente una vulnerabilidad.

27. 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 los servidores web
d. Reflective attack que afecta a algunos los servidores web

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

29. DMZ
a. Intranet.
b. Outranet.
c. Red perimetral.
d. Red privada virtual.

30. Ataque LAND
a. Generación con paquetes de origen y destino la misma máquina, para que los autoresponda.
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.

31. Si se hace un port stealing con ettercap con /10.10.200.40// /10.10.200.50//
a. Capturare todo el trafico entre las maquinas 10.10.200.40 y 10.10.200.50
b. Capturar todo el tráfico entre ambas máquinas, pero también su tráfico con otros equipos.
c. Capturare unicamente el trafico oneway de la 10.10.200.40 a la 10.10.200.50, pero no entre la 10.10.200.50 y la 10.10.200.50
d. Respuesta troll de la NSA.

32. Desde la maquina 10.10.102.200 se ejecuta y nos autenticamos como lsi ssh -P -L 10080:10.10.102.205:80 lsi@10.10.102.205
a. Nos conectamos a 10.10.102.200:10080 veremos el 80 de la 10.10.102.205
b. Nos conectamos a 10.10.102.205:10080 veremos el 80 de la 10.10.102.205
c. Nos conectamos a 10.10.102.200:10080 veremos la webcam de la esquina

del estadio de Riazor de A Coruña.
d. Ninguna de las anteriores es correcta.

33. En NTP la direccion 127.127.1.1
a. Indica que estamos utilizando un servidor de nivel superior para sincronizar el reloj de nuestro sistema
b. Indica que estamos utilizando un servidor de nivel inferior para sincronizar el reloj de nuestro sistema
c. Indica que estamo utilizando el reloj interno del equipo en cuestión.
d. No indica ninguna acción, simplemente se trata de una dirección IP de una máquina externa.

34. De forma general un proxy de tipo transparente.
a. Oculta la IP de origen
b. No oculta la IP de origen
c. No existen los proxies transparentes.
d. Ninguna de las anteriores es correcta.

35. Que afirmación es correcta.
a. Dist-upgrade únicamente se utiliza cuando queremos actualizar el sistema a una nueva distro.
b. Dist-upgrade nunca instalar nuevos paquetes, únicamente actualiza los existentes.
c. update se utiliza para instalar las actualizaciones de los paquetes.
d. Ninguna de las anteriores es correcta.

36. BPDU
a. 802.1Q
b. 802.1X
c. STP
d. X.509

37. ripemd-160
a. Simmetrico
b. Asimétrico
c. Híbrido
d. Hash

38. Usted realiza port scanning sobre una máquina y obtiene la siguiente tabla:
PORT STATE SERVICE
80/tcp open http
a) La máquina tiene un servidor web funcionando en el puerto 80
b) La máquina tiene filtrado de paquetes configurado
c) La máquina no tiene filtrado de paquetes configurado
d) Ninguna de las anteriores.

1. Indica la afirmación verdadera
a. La diferencia entre usar la red TOR o un Web-based proxy es que con Tor garantiza el cifrado extremo a extremo.
b. Hasta la fecha no se han reportado ataques sobre Tor
c. Para garantizar la seguridad de la red Tor, los Onion routers deben cambiar frecuentemente de IP y ubicación geográfica.
d. Todas las afirmaciones anteriores son falsas.

2. Si nuestra máquina está en un entorno conmutado.¿podemos obtener tráfico ajeno dirigido a otras máquinas?
a. Si, basta con activar el modo promiscuo de nuestra tarjeta de red.
b. Si, pero es necesario realizar un ataque de tipo MitM
c. Si pèro es necesario realizar algún ataque, aunque no tiene porque ser MitM
d. No, es imposible (salvo para la NSA).