

DNI

--	--	--	--	--	--	--	--	--	--

Convocatòria de la categoria de facultatiu/iva,
informàtica

Escala de suport del cos de Mossos
d'Esquadra

(núm. de reg. 007/002/22)

1a PROVA

1r Exercici

Test de coneixements

Data: 30 de març de 2023



1. Quin nivell de RAID no proveeix de fiabilitat addicional?

- a) RAID 1
- b) RAID 5
- c) RAID 0
- d) RAID 3

2. Quina és la mida màxima d'un fitxer i d'un volum en el sistema de fitxers NTFS?

- a) $2^{32} - 1$ bytes
- b) $2^{64} - 1$ bytes
- c) $2^{128} - 1$ bytes
- d) Les mides admeses es veuen afectades per la mida del clúster i el número de clústers per partició

3. Quin és l'avantatge d'utilitzar UDP respecte de TCP?

- a) UDP s'ha d'utilitzar quan les adreces IP del receptor no són conegudes
- b) UDP s'ha d'utilitzar sempre perquè és més ràpid i fiable que TCP
- c) UDP s'ha d'utilitzar quan és necessària una garantia en què l'ordre de les dades en el PC d'enviament coincideix en l'ordre d'arribada en el PC receptor
- d) UDP s'ha d'utilitzar quan la velocitat de transferència de les dades és més important que la correcció d'errors

4. Quines de les mesures de seguretat següents no corresponen a les mesures de nivell mig, proposades per la normativa de protecció de dades?

- a) Identificació i autenticació de les persones usuàries amb accés autoritzat
- b) Sistemes de xifrat en la transmissió de dades a través de la xarxa
- c) Control d'accés físic
- d) Auditoria (externa o interna) dels sistemes d'informació

5. Què és solidity?

- a) Un llenguatge orientat a objecte, utilitzat en la cadena de blocs (blockchain) per escriure contractes intel·ligents
- b) Una eina d'anàlisi d'arxius RAW
- c) Una eina d'anàlisi de memòria RAM
- d) Una eina d'anàlisi forense



6. Quina de les següents funcions hash estan lliures, a data d'avui, de col·lisions potencials:

- a) MD4
- b) SHA-512
- c) SHA-254
- d) MD5

7. Quina de les respostes següents és certa per a signatures digitals?

- a) L'emissor encripta el hash amb una clau pública
- b) L'emissor encripta el hash amb una clau privada
- c) L'emissor encripta el text pla amb una clau pública
- d) L'emissor encripta el text pla amb una clau privada

8. Quina comanda en Windows és equivalent a "cron" d'Unix/Linux?

- a) Schtasks
- b) Time
- c) Windows no té equivalència, s'ha de fer amb Shell Scripting
- d) Programer

9. Quin dispositiu opera a la Capa 2 (capa d'enllaç de dades) del model OSI?

- a) Hub
- b) Firewall
- c) Switch
- d) Router

10. Segons la Llei orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per a finalitats de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de sancions penals, el termini per a notificar a l'autoritat de protecció de dades d'una violació de la seguretat de les dades personals és de:

- a) 24 hores després de l'incident
- b) 24 hores després de conèixer l'incident
- c) 72 hores després de l'incident
- d) 72 hores després de conèixer l'incident



11. Quin dels següents és un tipus d'anàlisi estàtica?

- a) Comportament en temps d'execució
- b) Extracció de cadenes
- c) Direccionament de memòria
- d) Codificació de memòria

12. Segons el Decret 415/2011, de 13 de desembre, gestionar l'assignació d'usuaris i els perfils i nivells d'accés als sistemes d'informació de la Direcció General de la Policia, correspon a quina Àrea?

- a) Àrea d'Elaboració de Dades Policials
- b) Àrea de Coordinació de Projectes dels Sistemes d'Informació Policial
- c) Àrea de Seguretat en Tecnologies de la Informació
- d) Àrea Tècnica de Coordinació i Suport

13. Segons el principi de Kerckhoffs, quina de les afirmacions és correcta:

- a) El principi de Kerckhoffs també és conegut com a principi de disseny obert
- b) La seguretat per obscuritat no és un sistema fiable
- c) Tots els algorismes han de ser públics, només les claus són secretes
- d) Totes les anteriors són correctes

14. Senyaleu l'afirmació falsa. En un Mac amb chip T2, quan s'activa el FileVault:

- a) Tota la gestió de claus de FileVault es realitza en Secure Enclave
- b) L'enciptació dels dispositius d'emmagatzematge extern no utilitza les funcions de seguretat de Secure Enclave
- c) Tots els volums APFS es creen amb una clau d'enciptació de volum per defecte
- d) La clau de classe es protegeix amb una combinació de la contrasenya de l'usuari i l'UID de maquinari

15. Segons el model de referència OSI, quina de les capes següents és de tipus origen-destinació (o extrem a extrem):

- a) Capa d'enllaç
- b) Capa de xarxa
- c) Capa de sessió
- d) Capa de transport



16. Segons el RD 311/22, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat, a quin sistema que tracti dades de caràcter personal, no li serà aplicada la normativa següent:

- a) Reglament (UE) 2016/279
- b) Llei orgànica 3/2018, de 5 de desembre
- c) Llei orgànica 7/2021, de 26 de maig
- d) Directiva 95/46/CE (Reglament general de protecció de dades)

17. En un sistema d'arxius NTFS, quina és la mida màxima d'un registre de la MFT (Master File Table):

- a) 128 bytes
- b) 256 bytes
- c) 512 bytes
- d) 1024 bytes

18. En quina de les següents fases del procediment d'anàlisi forense, s'han de garantir les característiques d'admissible, autèntica, completa, creïble i confiable, de les evidències digitals?

- a) Preservació
- b) Adquisició
- c) Anàlisi
- d) Documentació

19. Segons Decret 289/2022, de 2 de novembre, el Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya, a través de la Secretaria de Telecomunicacions i Transformació Digital, depèn del Departament de:

- a) Presidència
- b) Polítiques Digitals i Administració Pública
- c) Interior
- d) Empresa i Treball

20. Segons el principi de Kerckhoffs, quin és el principi bàsic del sistema de xifrat?

- a) La seguretat del sistema depèn del secret de l'algorisme utilitzat
- b) La seguretat del sistema depèn de la clau utilitzada per xifrar i desxifrar els missatges
- c) La seguretat del sistema no és necessària si l'atacant no té accés a la clau privada
- d) La seguretat del sistema es basa a utilitzar un algorisme de xifrat robust



- 21. Segons la LO 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, quin dels següents no és un dret que la persona afectada pot exercir?**
- a) Dret a l'oblit
 - b) Dret de rectificació
 - c) Dret a la limitació del tractament
 - d) Dret d'accés
- 22. Les credencials, en el sistema operatiu Windows, s'emmagatzemen en el procés:**
- a) LSASS
 - b) Services
 - c) Netstat
 - d) Credsman
- 23. Segons l'article 459 de la Llei d'enjudiciament criminal, el reconeixement pericial es farà preferiblement:**
- a) Per un pèrit
 - b) Per dos pèrits
 - c) Per un pèrit públic
 - d) Per un pèrit privat i dos públics
- 24. Segons Decret 76/2020, de 4 d'agost, d'administració digital, quin dels eixos següents no forma part del model de ciberseguretat?**
- a) La gestió del risc
 - b) L'anàlisi de les ciberamenaces (ciber-intel·ligència)
 - c) La governança i l'estructura organitzativa
 - d) El control i la verificació
- 25. Què diferencia des del punt de vista arquitectònic el sistema operatiu OS X dels seus predecessors?**
- a) Que incorpora una nova interfície de finestres i el Wireport de sèrie
 - b) Que està basat en un comportament en xarxa
 - c) Que està basat en FreeBSD i és el primer que incorpora la interfície de línia d'ordres (terminal).
 - d) Que té compatibilitat amb plataformes Wintel



26. Quants clusters pot gestionar un sistema operatiu de 32 bits amb sistema de fitxers NTFS?

- a) $2^{16} - 1$
- b) $2^{32} - 1$
- c) $2^{64} - 1$
- d) $2^{128} - 1$

27. Quina d'aquestes distribucions LINUX està confeccionada per a l'anàlisi forense?

- a) CAINE
- b) SLAX
- c) MANJARO
- d) LG3D LiveCD

28. Quin protocol s'hauria de fer servir per a un servidor de streaming d'àudio, on és acceptable certa pèrdua d'informació?

- a) IP
- b) ICMP
- c) TCP
- d) UDP

29. Suposem un fitxer que conté adreces IP:

- a) L'adreça IP en sí no es considera dada personal, ja que per si sola no permet identificar a una persona física.
- b) El fitxer haurà de satisfer totes les mesures de seguretat de nivell alt proposades per la LOPDP.
- c) Caldrà sotmetre el fitxer a les mesures de seguretat proposades per la LOPDP.
- d) L'adreça IP es considera dada personal, però ja que per si sola no permet identificar a una persona física, no cal sotmetre els fitxers que les contenen a cap mesura de seguretat específica.

30. Segons la Guia de seguretat d'àrees crítiques per a la computació en el núvol de la CSA (Cloud Security Alliance), quin dels següents no és un model de desplegament:

- a) Públic
- b) Privat
- c) Híbrid
- d) Autoservei a demanda



31. Quin dels elements següents és una font potencial d'evidències de xarxa?

- a) Switch
- b) Router
- c) Firewall
- d) Mòdem

32. Amb què es codifica una adreça bitcoin convencional (P2PKH)?

- a) Base32Check
- b) Base58Check
- c) Base64Check
- d) Base256Check

33. Segons el Reglament (UE) 910/2014, el criteri que es refereix a un mitjà d'identificació electrònica, en el context d'un sistema d'identificació electrònica, que estableix un grau limitat de confiança en la identitat pretesa o declarada d'una persona i es descriu en referència amb les especificacions tècniques, les normes i els procediments d'aquest, entre altres els controls tècnics, i l'objectiu del qual és reduir el risc d'ús indegut o alteració de la identitat, fa referència al nivell de seguretat:

- a) Baix
- b) Substancial
- c) Alt
- d) Crític

34. Quina d'aquestes eines no està dissenyada per fer anàlisi forense?

- a) Encase
- b) X-Ways
- c) Paladine
- d) Spleuth Kit

35. Quina d'aquestes accions no pot evitar que Windows emmagatzemi un hash de la contrasenya d'administrador de LAN (LM) en Active Directory i bases de dades SAM locals?

- a) Implementar la directiva NoLMHash mitjançant directiva de grup
- b) Implementar la directiva NoLMHash editant el registre
- c) Implementar la directiva NoLMHash des de la interfície de línia d'ordres amb "cmdkey"
- d) Usar una contrasenya d'almenys 15 caràcters



36. En una arquitectura CISCA, quin són els modus de direccionament que suporta?

- a) Immediat
- b) Indirecte
- c) Relatiu
- d) Tots els anteriors són modus suportats

37. Segons la Llei d'enjudiciament criminal, en quin cas no s'haurà de sol·licitar autorització judicial prèvia a l'escorcoll de dispositius d'emmagatzematge massiu d'informació?

- a) En escorcoll domiciliari, amb manament judicial
- b) Quan els dispositius de la persona investigada es trobin fora del domicili
- c) En casos d'urgència amb interès constitucional legítim
- d) Quan s'hagi confiscat el dispositiu com a instrument del delictes

38. Quins són els noms de les capes en el model OSI, en ordre ascendent?

- a) Física, Enllaç de dades, Transport, Xarxa, Sessió, Presentació, Aplicació
- b) Física, Xarxa, Enllaç de dades, Transport, Sessió, Presentació, Aplicació
- c) Física, Enllaç de dades, Xarxa, Transport, Sessió, Presentació, Aplicació
- d) Física, Enllaç de dades, Xarxa, Transport, Presentació, Sessió, Aplicació

39. Quina és la principal diferència entre un sistema de xifrat de clau pública i un de clau privada?

- a) Un sistema de xifrat de clau pública utilitza una clau diferent per xifrar i desxifrar mentre que un de clau privada utilitza la mateixa clau
- b) Un sistema de xifrat de clau pública és utilitzat per garantir la privacitat mentre que un de clau privada és utilitzat per garantir la confidencialitat
- c) Un sistema de xifrat de clau pública s'utilitza per garantir l'autenticitat mentre que un de clau privada és utilitzat per garantir la confidencialitat
- d) Un sistema de xifrat de clau pública és utilitzat per garantir la privacitat mentre que un de clau privada és utilitzat per garantir l'autenticitat

40. En el fitxer de contrasenyes d'un sistema UNIX, quin enunciat és incorrecte:

- a) Si dos usuaris tenen la mateixa contrasenya, apareixeran xifrades de la mateixa manera en el fitxer de contrasenyes.
- b) L'algorisme de xifrat de les contrasenyes es basa en el criptosistema DES.
- c) Per a cada contrasenya, en el moment de xifrar-la, es poden produir 4.096 codificacions possibles.
- d) El fitxer /etc/passwd té permís de lectura per a totes les persones usuàries.



41. Què és necessari per falsificar una signatura digital?

- a) Accés a la clau privada de la persona que ha generat la signatura
- b) Utilitzar tècniques criptogràfiques avançades
- c) Tenir accés a un certificat digital emès per una entitat de confiança
- d) Una signatura digital no es pot falsificar si s'utilitza un algorisme robust

42. En una arquitectura CISCA, quin dels següents no és un tipus de registres del processador (CPU)?

- a) De desbordament (overflow)
- b) De propòsit general
- c) D'accés a memòria
- d) D'estat i de control

43. En una classificació, segons la varietat d'operacions, d'un sistema xifrat homomòrfic, quina d'aquestes categories no pertany a un sistema de classificat segons les seves propietats i varietat d'operacions que es poden fer sobre les seves dades?

- a) Somewhat Homomorphic
- b) Levelled Homomorphic
- c) Fully Homomorphic
- d) Half Homomorphic

44. Segons el NIST Definition of Cloud Computing, quines d'aquestes opcions no és un model de servei en el núvol?

- a) Infraestructura com a servei (IaaS)
- b) Sistema com a servei (SaaS)
- c) Xarxa com a servei (NaaS)
- d) Plataforma com a servei (PaaS)

45. Segons l'informe IOCTA d'Europol, quin dels següents no forma part dels crims ciber-dependents?

- a) El Ransomware
- b) Els atacs DDoS
- c) Els Continguts Sexuals d'Explotació infantil
- d) El Malware en els dispositius mòbils



46. Segons l'article 457 de la Llei d'enjudiciament criminal, els pèrits no titulars són:

- a) Els que no tenen títol oficial però tenen coneixement o pràctiques especials en alguna ciència o art
- b) Els que no han estat inscrits en la relació que elabora l'Administració de Justícia
- c) Els privats que proposa la defensa
- d) Els privats que proposa l'acusació

47. En una CPU de propòsit general amb arquitectura CISCA, quin d'aquests senyals és de sortida en la Unitat de control (UC)?

- a) Temporització
- b) Control de la unitat aritmètica i lògica (ALU)
- c) Registre d'instrucció (IR)
- d) Registre d'estat

48. Quin d'aquests arxius d'un sistema operatiu Linux guarda els inicis de sessió fallits o erroris?

- a) /var/run/utmp
- b) /var/log/secure
- c) /var/log/btmp
- d) /var/log/wtmp

49. Quina longitud té el hash d'una adreça de bitcoins convencional (P2PKH)?

- a) 16 bytes
- b) 20 bytes
- c) 26 bytes
- d) 32 bytes

50. Quina de les següents és un objectiu de la capa de transport en el model OSI?

- a) El lliurament salt a salt de paquets d'una xarxa a una altra
- b) La representació de les dades en una estructura que pot ser entesa per processos en els terminals
- c) L'encapsulament dels paquets IP per transportar
- d) L'assegurança de la transferència fiable de dades



PREGUNTES DE RESERVA

51. Quina de les següents afirmacions és falsa en relació amb els algorismes de Hash?

- a) Accepten entrades de longitud fixa i genera un valor de longitud variable
- b) No és necessària una clau
- c) És semblant a les funcions CRC
- d) Crea una empremta (fingerprint) del missatge

52. Quin és el tipus de partició de disc en què s'assigna noms d'unitats com C:, E: o X:?

- a) Extesa
- b) Física
- c) Lògica
- d) Virtual

53. Els permisos de fitxers en UNIX, consisteixen en quin dels següents tres tipus?

- a) Modificació, lectura i execució
- b) Lectura, escriptura i execució
- c) Control total, només lectura i execució
- d) Escripura, lectura i obertura

54. En seguretat informàtica, quina de les següents propietats protegeix de modificacions a les dades?

- a) Confidencialitat
- b) Integritat
- c) Disponibilitat
- d) Auditable

55. Quin dels següents sistemes de fitxers emmagatzema, per a cada fitxer, la data i hora del darrer accés?

- a) NTFS
- b) FAT 12
- c) FAT 16
- d) FAT 32

Convocatòria de la categoria de facultatiu/iva,
informàtica

Escala de suport del cos de Mossos
d'Esquadra

(núm. de reg. 007/002/22)

**PLANTILLA DE
CORRECCIÓ**

1a PROVA

1r Exercici

Test de coneixements

Data: 30 de març de 2023



**Convocatòria de la categoria de facultatiu/iva, informàtica
(núm. de reg. 007/002/22)**

Pregunta	Resposta correcta
1	c
2	d
3	d
4	b
5	a
6	b
7	b
8	a
9	c
10	d
11	a
12	c
13	d
14	b
15	d
16	d
17	d
18	b
19	a
20	b
21	a
22	a
23	b
24	b
25	c
26	b
27	a
28	d
29	c
30	d



**Convocatòria de la categoria de facultatiu/iva, informàtica
(núm. de reg. 007/002/22)**

Pregunta	Resposta correcta
31	c
32	b
33	a
34	d
35	c
36	d
37	c
38	c
39	a
40	d
41	a
42	a
43	d
44	c
45	c
46	a
47	b
48	c
49	b
50	d
Preguntes de reserva	Resposta correcta
51	a
52	c
53	b
54	b
55	a