Generalitat de Catalunya
Departament d'Interior
Direcció General de la Policia

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

2n Exercici

Supòsit pràctic tipus test

Data: 30 de març de 2023

Un operatiu policial, on vostè participa com assessor en matèria forense, es troba en un domicili per realitzar una perquisició. Es cerquen evidències digitals que ajudin a la investigació del delicte i la recopilació de proves.

Quan comença l'escorcoll, es troba un ordinador encès amb Windows 11 instal·lat i sense bloqueig de pantalla.

S'intervenen els dispositius següents per fer una anàlisi pericial en el laboratori:

- **Ordinador amb sistema operatiu Windows 11 (ordinador encès)**
- **Ordinador MacBook Air amb xip T2**
- **Telèfon mòbil amb sistema operatiu Android i xipset (chipset) Qualcomm**
- **Telèfon mòbil amb sistema operatiu Android 12**
- **Telèfon mòbil amb sistema operatiu Android 13**

Responeu a les preguntes següents:

1. **Quina d'aquestes dades volàtils s'ha de recollir primer en l'ordinador encès, segons les diferents recomanacions, entre les quals les del US National Institute of Standards and Technology (NIST):**

   a) Processos en execució.
   b) Connexions de xarxa.
   c) Contingut de la RAM.
   d) Sessions iniciades (amb login).

2. **Amb quina d'aquestes tècniques no es pot fer un buidatge físic de la memòria del telèfon mòbil amb Android i xipset (chipset) Qualcomm que està bloquejat amb contrasenya desconeguda:**

   a) EDL (Emergency Download Mode)
   b) JTAG (Join Test Action Group)
   c) ADB (Android Debug Bridge)
   d) Chip-off (treure el xip)

3. Si se sap que un dels telèfons disposa del sistema operatiu Android 12, per defecte trobarem les dades a memòria:

a) Xifrades amb FBE (File Based Encryption).
b) Xifrades amb FDE (Full Disk Encryption).
c) Sense xifrar si la persona usuària no ha utilitzat cap sistema de bloqueig del terminal.
d) Sense xifrar si la persona usuària no va activar el xifrat durant la configuració inicial per utilitzar el telèfon.

4. Es vol extreure la base de dades de WhatsApp desxifrada del telèfon mòbil amb el sistema operatiu Android 13. La contrasenya d'accés al telèfon és coneguda. Quin tipus d'extracció mínima ens ho permet fer?

a) Lògica.
b) Lògica avançada.
c) Física.
d) Sistema de fitxers.

5. Quina acció de seguretat és recomanable realitzar quan es fa el clon d'un dispositiu?

a) Muntar el dispositiu de destí en OW.
b) Realitzar un *wipe* al dispositiu de destí.
c) Muntar el dispositiu origen en OW.
d) Realitzar un *wipe* al dispositiu d'origen.

6. Quina d'aquestes eines no serveix per desxifrar la contrasenya d'usuari de Windows (NTLM) de l'ordinador un cop apagada la màquina:

a) NTMLCrack
b) RainbowCrack
c) OphCrack
e) John the Reaper

7. Ens demanen saber quantes vegades s'ha executat una aplicació de "*command and control*" coneguda en el sistema i les dates en què s'han fet. En quina carpeta de Windows es pot trobar la informació?

a) AppData
b) AccessChk
c) Prefetch
d) MostRecentFiles

8. Ens demanen trobar alguna evidència que indiqui si una persona usuària va copiar un arxiu de l'ordinador (SO Windows) a una memòria USB externa en una data determinada. On es pot trobar aquesta informació?

a) Shellbag
b) Info2
c) Prefetch
d) MostRecentFiles

9. Es disposa d'una llicència de sistema amb el programari adequat per llençar atacs per esbrinar la contrasenya d'un disc xifrat amb BitLocker que estava dins la màquina amb Windows. Per motius d'eficiència i rapidesa s'ha decidit llogar un servei de maquinari al núvol. Quin servei s'ha de contractar?

a) Infrastructure as a service (IaaS)
b) Morphing as a service (MaaS)
c) Platform as a service (PaaS)
d) Software as a service (SaaS)

10. Si volem fer una adquisició forense de la SSD del MacBook Air amb xip T2 ens trobarem que:

a) La informació esta xifrada per defecte.
b) La informació només es pot adquirir en mode d'arrancada segura.
c) La informació mai no es pot adquirir.
d) La informació està sense xifrar.

PREGUNTES DE RESERVA:

11. Es demana generar una imatge forense del disc de l'ordinador amb compressió. Quin tipus d'arxiu no podem fer servir?

a) E01
b) AFF4
c) RAW
d) WIM

12. Ens interessa saber si l'equip que està encès està suplantant una adreça IP. On la busca?

a) Winincfg
b) Ipconfig
c) Iptables
d) Trumpet winsock

Generalitat de Catalunya
Departament d'Interior
Direcció General de la Policia

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

2n Exercici

Supòsit pràctic tipus test

Data: 30 de març de 2023

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

Pregunta	Resposta correcta
1	b
2	c
3	a
4	c
5	b
6	a
7	c
8	a
9	a
10	a

Pregunta de reserva	Resposta correcta
11	c
12	b