Prova Final UF1 Seguretat

OPENSSL

1.-(2pts) a) Escriu un missatge en un arxiu de text i xifra'l simètricament amb *openssl* fent servir l'algoritme AES-192-CBC i una determinada "passphrase"

aII) Escriu el valor de la "passphrase" utilitzada l'apartat anterior en un altre arxiu de text (sense indicar cap salt de línia al final!) i xifra aquest altre arxiu de text amb aquesta clau pública (pertanyent al professor).

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwVAHDRiWF7gq8NRIBzbV
HrbTJdY+B7A1rDOHJSE9xQAt162Kw3x7y+m7RWduROuDIxP5VpqHOk9jhBJOPDCq
v9j1jlIVxlUab4SlhHXvtHHVYI7i+MI0IpFlPdWOyJEB977MCblvnRO9gZik+xbg
rpgzx38cNQ4AhpNSYffzkWydTHJpM1+8YPv1hUsgCps5/VJaCvX3flU6AeGtnBy9
2R7nd+TJPNVylURH7k0TupHvJ7eVMg/myiZrwzM/qzfucv5mL03iG+ztnYefXDIQ
b/kO952ksmFE3Z+O4iSXfwKm+tvOHTRMplXgJqM6PpCcXWTk66NFVhuaT2mYJY2W
hQIDAQAB
-----END PUBLIC KEY-----

Entrega **el fitxer contenint el missatge secret** (xifrat simètricament) i **el fitxer contenint la "passphrase"** emprada per generar el fitxer anterior (xifrada asimètricament). El professor haurà de ser poder desxifrar la "passphrase" amb la seva clau privada i, un cop coneguda, fer servir aquesta "passphrase" per desxifrar llavors aquest missatge xifrat rebut.

XIFRATGE DE CARPETES I FITXERS

2.-(1pt) Escriu un missatge en un arxiu de text i xifra'l mitjançant *age* amb la següent clau pública (pertanyent al professor): *age127r264lu0625jaste9rdjneldgh5pyfm5terwlurlqcgy2u0ra5sc3cx93* Entrega el **fitxer xifrat** (el professor haurà de poder desxifrar-lo amb la seva clau privada)

LUKS

3.-(2pts) Prepara un fitxer de 100MB com a disc "loop" formatejat en Ext4 i fes que sigui de tipus LUKS. Munta'l, guarda-hi allà un fitxer de text amb un determinat missatge al seu interior i desmunta'l. Tot seguit afegeix una segona clau al dispositiu LUKS anterior, la qual ha de consistir en un fitxer contenint una tira binària aleatòria de 10 bytes. Entrega tant aquest **fitxer-clau binari** com el propi **disc LUKS** (el professor haurà de poder accedir, gràcies al fitxer-clau, a l'interior del dispositiu LUKS i llavors observar el missatge secret guardat al seu interior.)

METADADES

4.-(1pt) Descarrega't el fitxer PDF que t'haurà proporcionat el professor i:

a) Esbrina el software original amb el què s'ha confeccionat el document i la seva data de creació. Entrega les **captures necessàries** on es vegi l'execució de la comanda que has executat i el resultat obtingut

b) Elimina totes les metadades que puguis. Entrega les **captures necessàries** on es vegi l'execució de la comanda que has executat i el resultat obtingut

ESTEGANOGRAFIA

5.-(2pts) a) Troba el missatge incrustat (que tindrà la forma "*flag{...}*") dins de cadascuna de les tres fotografies proporcionades pel professor emprant algun dels mètodes vistos a classe (comandes *strings/hexdump*, comandes *binwalk/dd*, comanda *exiftool*, edició digital...). Entrega les **captures necessàries** on es vegi l'execució de les comandes que has executat en cada cas i els resultats obtinguts

b) Utilitza la comanda *steghide* per ocultar un missatge secret dins d'una imatge JPG qualsevol que tinguis al teu sistema. Fes servir com a contrasenya "1234". Entrega la **imatge JPG resultant** (el professor haurà de poder obtenir aquest missatge secret sense problema)

CARVING

6.-(2pts) a) Descarrega't el fitxer "disk.tar.xz" que t'haurà proporcionat el professor i descomprimeix-lo. El fitxer binari resultant conté dins el seu interior una sola fotografia PNG (esborrada). Extreu-la mitjançant *dd* sabent que el "magic number" d'inici de les imatges PNG és *89 50 4e 47 0d 0a 1a 0a* i el "magic number" de final és *49 45 4E 44 AE 42 60 82* Entrega les **captures necessàries** on es vegi l'execució de les comandes que has executat i **la fotografia extreta**

NOTA: No ho intentis amb Photorec o *binwalk* perquè perdràs el temps: no funcionen en aquest cas

b) Descarrega't el fitxer "memdumpExamen.tar.xz" que t'haurà proporcionat el professor i descomprimeix-lo. Aquest fitxer representa una part d'una captura de la memòria RAM d'un ordinador en un determinat instant. Troba-hi, fent servir *bulk_extractor*, el domini més visitat i l'adreça de correu electrònic més emprada. Entrega les **captures necessàries** on es vegi l'execució de la comanda que has executat i el resultat obtingut