

# Certified Offensive and Defensive Security Professional

**Nombres y Apellidos:** \*\*\*\*\*

**Documento de Identidad:** \*\*\*\*\*

## Solucionario: Reto Informático numero 1

**Respuestas:** liverpool123

**Enunciado de ejemplo:** se tiene el siguiente servidor web. Este sería un buen lugar para obtener la bandera numero 1:

Ip server web  
<http://52.90.59.125/>

**Hash Encontrado:** E1A04996A37395FCD9C7B7C5286270F7

**Respuesta hash crackeado:** liverpool123

**Documentación del reto:** para este reto se utilizó la herramienta dirb junto con el diccionario wordlists/common.txt para poder escanear la página con las posibles urls ocultas, como no se encontró ninguna se identificó el servidor con una consulta por telnet al puerto 80 obteniendo un servidor Apache/2.4.29 (Ubuntu) luego se utilizó el dirb con wordlists/vulns/apache.txt sin éxito, luego se probó el dirb con wordlists/medium.txt encontrando un directorio en webadmin con el archivo crackeame.txt donde se encontró una cadena hexadecimal de 32 caracteres. Se utilizó la herramienta online <https://crackstation.net/> identificando el hash como md5

## Solucionario: Reto Informático numero 2

**Respuestas:** gunsandroses

**Enunciado:** se tiene el siguiente servidor WEB Y URL

<http://52.90.59.125/>

**Hash Encontrado:**

d3bf679621db5a9b7bc6774af584082065dd9c7f22af5f1edd126c4bb70b5b94

**Respuesta hash crackeado:** gunsandroses

**Documentación del reto:** Al observar el código fuente de la página en el anterior reto se pudo observar el hash a crackear.

```
<!-- ESTE ES UNA CONTRASEÑA CIFRADA, TE VENDRIA BIEN DESCIFRARLA PARA  
OBTENER LA BANDERA 2  
d3bf679621db5a9b7bc6774af584082065dd9c7f22af5f1edd126c4bb70b5b94  
-->
```

El hash es de longitud de 64 caracteres en hexadecimal posiblemente un hash sha256. Al probar el hash con la herramienta online <https://crackstation.net> se confirmó el tipo de hash sha256 y se obtuvo la respuesta gunsandroses

### **Solucionario: Reto Informático numero 3**

**Respuestas:** mrrobot, otinasug123

**Enunciado:** se tiene la siguiente url  
<http://52.90.59.125//steganography/>

**base64 Encontrado 1:** bXJyb2JvdA==

**Respuesta base64 crackeado 1:** mrrobot

**Hash 1:** 77D95504A8B987424EA0391B0D920F6D

**Respuesta hash 1 crackeado:** otinasug123

**Documentación del reto:** se observó una página con una imagen en blanco y negro y un texto posiblemente cifrado con base64 (posiblemente la contraseña para descifrar los datos ocultos por steganografía en la imagen), se utilizó la herramienta CyberChef <https://gchq.github.io/CyberChef/> para tratar de descifrar el texto y se obtuvo mrrobot. Luego se utilizó la herramienta Camouflage desde un S.O. Windows XP con la contraseña encontrada y se obtuvieron 2 archivos una imagen steganogra.png y un archivo oculto.txt con la cadena hash 77D95504A8B987424EA0391B0D920F6D. Se utilizó la herramienta hashcat con la regla best64.rule y los diccionarios rockyou.txt y realhuman\_phill.txt:

```
hashcat -m 0 -D 1 -w 3 oculto.txt rockyou.txt realhuman_phill.txt -r best64.rule --debug-mode=1  
--debug-file=foundrule.rule
```

### **Solucionario: Reto Informático numero 4**

**Respuestas:** ecuaestilolatino, Ecuaestilolatino, ECUAESTILOLATINO, onitalolitseauce, ecuaestilolatino99, 1ecuaestilolatino

**Enunciado:** Se tienen los 6 hashes:

**Hash 1:** 89337CF7FAFB6110A2C72E5AA711639E5F3F37E2

**Respuesta hash 1 crackeado:** ecuaestilolatino

**Hash 2:** 16BD2368D9E7789B28BEB978D394B4EED8DE8641

**Respuesta hash 2 crackeado:** Ecuaestilolatino

**Hash 3:** F0F84313C7ADA13F4DDA289DDC683EEF41E83185

**Respuesta hash 3 crackeado:** ECUAESTILOLATINO

**Hash 4:** E9045AE52E2CA70232C5678F506CA3ECE9C7BAA0

**Respuesta hash 4 crackeado:** onitalolitseauce

**Hash 5:** 54D5F411F4ADA02512E69B81CC68EF28F9D83940

**Respuesta hash 5 crackeado:** ecuaestilolatino99

**Hash 6:** 9D0C2FC4A62F8846433799533720C5C43B0A0414

**Respuesta hash 6 crackeado:** 1ecuaestilolatino

**Documentación del reto:** se observan 6 hashes de 40 caracteres de longitud en hexadecimal y se prueba a descifrar cada hash con la herramienta online <https://crackstation.net> encontrando

descifrar solo 2 hashes de tipo sha1. Para los 4 hashes restantes se utilizó la herramienta hashcat con los diccionarios rockyou.txt, realhuman\_phill.txt y los siguientes comandos:

```
hashcat -m 100 -D 2 -w 3 hash.txt rockyou.txt realhuman_phill.txt  
hashcat -m 100 -D 2 -w 3 hash.txt rockyou.txt realhuman_phill.txt -r best64.rule --debug-mode=1 --debug-file=foundwithrule.rule
```

#### **Solucionario: Reto Informático numero 5**

**Respuestas:** usuario pablo y contraseña letmein

**Enunciado:** Se tiene el siguiente archivo reto5.cap, debes de extraer los usuarios y password de protocolos de red que no requieren autenticación.

**Documentación del reto:** se abre el archivo .cap con la herramienta wireshark y se observa una comunicación el protocolo HTTP, se sigue ese flujo y se encuentra un login correcto por POST con el usuario pablo y la contraseña letmein

#### **Solucionario: Reto Informático numero 6**

**Respuestas:** B@T+3n, =\$P1rm, AA99a2, 236699852147, 012345678900, 11119999333

**Enunciado:** Se tienen los siguientes hashes, hay que tratar de romperlos:

**Hash 1:** 61DA2C8562576685719DC8FA1DCA0E62

**Respuesta hash 1 crackeado:** B@T+3n

**Hash 2:** 51BD4343528792C4BADF734D2119391B

**Respuesta hash 2 crackeado:** =\$P1rm

**Hash 3:** 2E3C180811AD56EAF8FD69A6D8E30F9

**Respuesta hash 3 crackeado:** AA99a2

**Hash 4:** CB6E05C7FCF884621951883C77005BD1

**Respuesta hash 4 crackeado:** 236699852147

**Hash 5:** 64D791D55E366146C39367631B5AF31B

**Respuesta hash 5 crackeado:** 012345678900

**Hash 6:** 343BFABA861604E67E4B70D0D36BD0F7

**Respuesta hash 6 crackeado:** 11119999333

**Documentación del reto:** se observan 6 hashes de 32 caracteres de longitud en hexadecimal y se prueba a descifrar cada hash con la herramienta <https://www.objectif-securite.ch/ophcrack> y se encontraron todas las contraseñas.

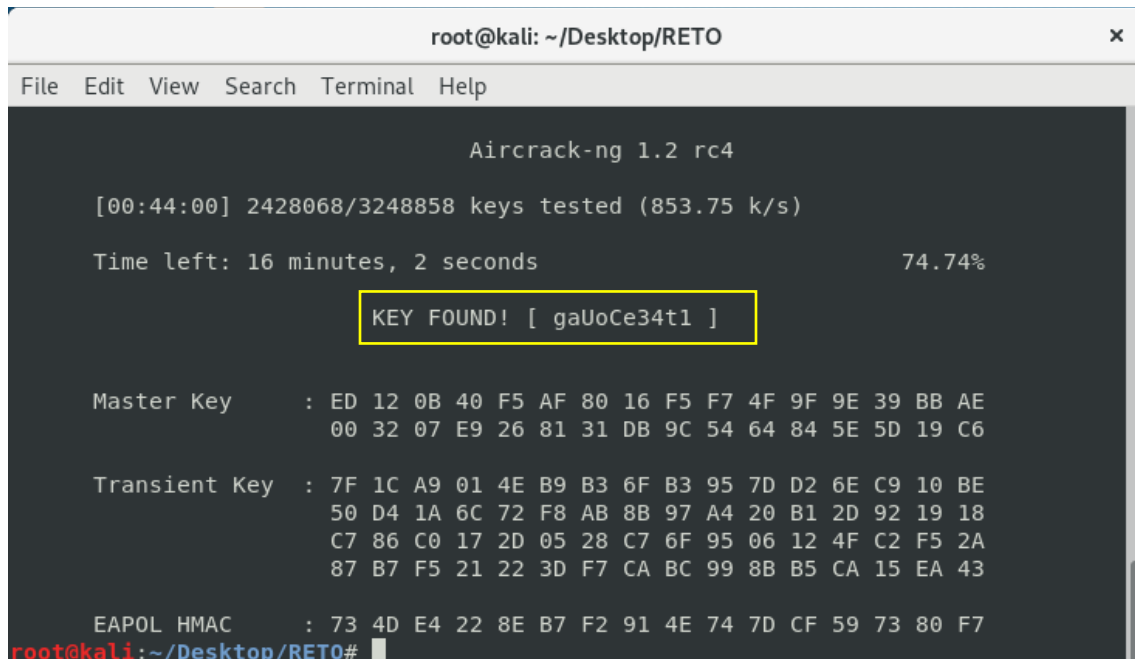
#### **Solucionario: Reto Informático numero 7**

**Respuestas:** gaUoCe34t1

**Enunciado:** Se tienen los siguientes 2 archivos: Tramared.cap & dicc.txt

**Respuesta key crackeada:** gaUoCe34t1

**Documentación del reto:** se abre el archivo .cap con la herramienta wireshark y se observa una comunicación el protocolo 802.11. Se utilizó la herramienta aircrack-ng y el diccionario dicc.txt junto con la dirección mac identificada del access point 18:d6:c7:3f:23:89 con el comando: aircrack-ng -w dicc.txt -b 18:d6:c7:3f:23:89 tramared.cap y después de 44 minutos se encontró la clave gaUoCe34t1

A screenshot of a terminal window titled 'root@kali: ~/Desktop/RETO'. The terminal shows the output of the 'aircrack-ng 1.2 rc4' command. It displays progress information: '[00:44:00] 2428068/3248858 keys tested (853.75 k/s)' and 'Time left: 16 minutes, 2 seconds' with a progress bar at 74.74%. A yellow box highlights the text 'KEY FOUND! [ gaUoCe34t1 ]'. Below this, the 'Master Key' and 'Transient Key' are shown in hexadecimal, followed by the 'EAPOL HMAC'. The prompt 'root@kali:~/Desktop/RETO#' is visible at the bottom.

```
root@kali: ~/Desktop/RETO
File Edit View Search Terminal Help

Aircrack-ng 1.2 rc4

[00:44:00] 2428068/3248858 keys tested (853.75 k/s)

Time left: 16 minutes, 2 seconds 74.74%

KEY FOUND! [ gaUoCe34t1 ]

Master Key      : ED 12 0B 40 F5 AF 80 16 F5 F7 4F 9F 9E 39 BB AE
                  00 32 07 E9 26 81 31 DB 9C 54 64 84 5E 5D 19 C6

Transient Key   : 7F 1C A9 01 4E B9 B3 6F B3 95 7D D2 6E C9 10 BE
                  50 D4 1A 6C 72 F8 AB 8B 97 A4 20 B1 2D 92 19 18
                  C7 86 C0 17 2D 05 28 C7 6F 95 06 12 4F C2 F5 2A
                  87 B7 F5 21 22 3D F7 CA BC 99 8B B5 CA 15 EA 43

EAPOL HMAC     : 73 4D E4 22 8E B7 F2 91 4E 74 7D CF 59 73 80 F7
root@kali:~/Desktop/RETO#
```

**Solucionario:** Reto Informático numero 8

**Respuestas:** MAZINGERLISTO2020

**Enunciado:** Se tienen dos archivos: un archivo cifrado, y una llave criptográfica.

**Respuesta key crackeada:** MAZINGERLISTO2020

**Documentación del reto:** desde kali Linux se utiliza la herramienta openssl con el comando: openssl rsautl -decrypt -in bandera8cifrada.txt -inkey privadacert.txt -out mi\_archivo\_decifrado y se coloca la contraseña obtenida del reto anterior gaUoCe34t1 para obtener el texto MAZINGERLISTO2020 en el archivo mi\_archivo\_decifrado

**Solucionario:** Reto Informático numero 9

**Respuesta Hash 1 Obtenido:** 50A370199AA13131DEA546CEFEC233C6  
**Respuesta Hash 2 Obtenido:** F7247211BEA358BF5D8D44130EDDB3CB  
**Respuesta Hash 3 Obtenido:** 76AA211D3C67CCA1F84EC12F9225067C  
**Respuesta Hash 4 Obtenido:** 43B36CA2C59434925CD83A2B21B000D2  
**Respuesta Hash 5 Obtenido:** C420F35DB4C65685A08787A703065759  
**Respuesta Hash 6 Obtenido:** AADFCBD95C8C096472D98742227F36F9  
**Respuesta Hash 7 Obtenido:** DBC54C6A87719181BF21631CB2C17964

**Enunciado:** Se tienen una copia (Backup) cifrada de un sistema firewall perimetral, debes de proceder a cargarla al respectivo firewall.

**Documentación del reto:** hay varias formas de solucionar este reto, la utilizada fue la siguiente por ser la más rápida. Primero se eliminó la primera y última línea del archivo encriptado

---- BEGIN config.xml ----

---- END config.xml ----

- Luego desde la consola podemos desencriptar el archivo con openssl (primero desencriptará el base64 y luego el aes-256-cbc) y colocamos la contraseña MAZINGERLISTO2020 obtenida del reto anterior:

```
openssl enc -aes-256-cbc -base64 -d -p -in config-firewallcodsp-CIFRADO.xml -out config-dec.xml
```

- Por ultimo al observar el nodo rule seguido del atributo interface con valor lan se guardó el valor de la descripción (las 2 primeras estaban vacías).

**Solucionario:** Reto Informático numero 10

**Respuestas:** Danacanty, Jesus8892, 0135445216, berzuit2286, kliplev, phillipkingforever y yo3165867463

**Enunciado:** Reventar (Crackear) los 7 hashes (Password) obtenidos en el reto número 9.

**Hash 1:** 50A370199AA13131DEA546CEFEC233C6

**Respuesta hash 1 crackeado:** Danacanty

**Hash 2:** F7247211BEA358BF5D8D44130EDDB3CB

**Respuesta hash 2 crackeado:** Jesus8892

**Hash 3:** 76AA211D3C67CCA1F84EC12F9225067C

**Respuesta hash 3 crackeado:** 0135445216

**Hash 4:** 43B36CA2C59434925CD83A2B21B000D2

**Respuesta hash 4 crackeado:** berzuit2286

**Hash 5:** C420F35DB4C65685A08787A703065759

**Respuesta hash 5 crackeado:** kliplev

**Hash 6:** AADFCBD95C8C096472D98742227F36F9

**Respuesta hash 6 crackeado:** phillipkingforever

**Hash 7:** DBC54C6A87719181BF21631CB2C17964

**Respuesta hash 7 crackeado:** yo3165867463

**Documentación del reto:** se identificó cada hash como md5, luego se procedió a utilizar la herramienta hashcat para desencriptarlos con el comando:

```
hashcat -m 0 -D 1 -w 3 hash.txt rockyou.txt realhuman_phill.txt -r best64.rule --debug-mode=1 --debug-file=rulesused.rule
```

**Solucionario:** Reto Informático numero 11

**Solucionario:** Reto Informático numero 12

**Respuestas:** brujadel71brujadel71, ¿?

**Enunciado:** Construir un diccionario con los personajes de la famosa serie de televisión mexicana el chavo del ocho. Una vez que se construye el diccionario en mención, crear una regla personalizado con los primeros 12 items de las reglas de la aplicación hashcat (Implemented compatible functions)  
[https://hashcat.net/wiki/doku.php?id=rule\\_based\\_attack](https://hashcat.net/wiki/doku.php?id=rule_based_attack)

Luego debes de romper (Crackear) los siguientes hash:

DEDB6F3A8CDBD055AB3710890EB1D974 (MD5)  
2427f3d7e91d20e31a2ee49607bd189144559886 (SHA1 - SHA128)

**Hash Encontrado 1:** DEDB6F3A8CDBD055AB3710890EB1D974

**Respuesta hash crackeado 1:** brujadel71brujadel71

**Hash Encontrado 2:** 2427f3d7e91d20e31a2ee49607bd189144559886

**Respuesta hash crackeado 2:** ¿?

**Documentación del reto:** Se creó un diccionario a partir de los nombres mencionados en [https://es.wikipedia.org/wiki/El\\_Chavo\\_del\\_8](https://es.wikipedia.org/wiki/El_Chavo_del_8) con la herramienta hashcat y se crackeo el primer hash (identificado como md5) con el siguiente comando:

```
hashcat -m 0 -D 1 DEDB6F3A8CDBD055AB3710890EB1D974 dic.txt -r rules.txt --debug-mode=1  
--debug-file=foundWithRule1.txt
```

```
hashcat -m 100 -D 1 2427f3d7e91d20e31a2ee49607bd189144559886 dic.txt -r rules.txt --  
debug-mode=1 --debug-file=foundWithRule2.txt
```

El archivo rules.txt contenía las siguientes reglas (se colocaron reglas adicionales para crackear):

```
:  
!  
u  
c  
C  
t  
T1  
T2  
r  
d  
p1  
p2  
sa@  
sa4  
se3  
so0  
sl1
```

## Solucionario: Reto Informático numero 13

### Respuestas

IP Agresor Informático: 201.233.17.174

Nombre Malware (Ejecutado) por el agresor: kjkabuto.exe

Puerto Origen conexión Malware: 4815

Puerto Destino por donde entro el malware a la victima: 3389

PID del malware: 2728

Firma del malware antivirus MICROSOFT (Virus total): Trojan:Win64/Meterpreter.B

Hash del Malware MD5: 590eb099ec4833d72da64b9573f527ce

Hash del Malware SHA1: 8927b1ab1762ee387fb51d7a21a75b7c6423ed0a

IP donde se conectan a la victima pro el RDP: 172.31.55.117

Ruta donde se infecto el malware en el equipo victima:

C:\Users\Administrator\Downloads\kjkabuto.exe

**Enunciado:** Se tiene un volcado de memoria RAM, el cual es resultante de una investigación forense digital, y hace parte de una prueba forense. Respecto a este dump (volcado de memoria) se debe de obtener lo siguiente:

- A tener en cuenta: (El volcado de memoria está localizado en la carpeta reto 13 y se llama: memserver.mem)

**Documentación del reto:** se utilizó la herramienta volatility para la obtención de la información:

- observamos el perfil del volcado

```
volatility imageinfo -f "memserver.mem"
```

- se encontró un perfil de Windows 10, luego se listaron los procesos encontrando 1 archivo con nombre sospechoso "kjkabuto.exe" con PID 2728:

```
volatility --profile=Win10x64_14393 -f memserver.mem pslist
```

- al observar el historico de comandos vemos que el archivo se ejecuto desde la carpeta Downloads del usuario Administrator:

```
volatility --profile=Win10x64_14393 -f memserver.mem cmdline
```

- al examinar las conexiones establecidas remotamente vemos una conexión hacia el escritorio remoto:

```
volatility --profile=Win10x64_14393 -f memserver.mem netscan | findstr "ESTABLISHED" | findstr /V "127.0.0.1:"
```

- encontrando la conexión establecida hacia el escritorio remoto

172.31.55.117:3389 201.233.17.174:4815

- por ultimo dumpeamos el contenido del archivo en un ejecutable para analizarlo por virustotal:

volatility --profile=Win10x64\_14393 -f memserver.mem" procdump -p 2728 --dump-dir .

### **Solucionario: Reto Informático numero 14**

### **Solucionario: Reto Informático numero 15**

**Respuestas:** dajuan90, mar8ia, megatron8M+, OPTi44\*-

**Enunciado:** Se tienen los siguientes hashes. Proceder a romperlos

**Hash Encontrado 1:** f99452d280d7310e26ba2362cfc62ae2f090a7b1

**Respuesta hash crackeado 1:** dajuan90

**Hash Encontrado 2:**

810F91EBBD575F21C07C60B1866D6BE309503388366DECD165D74A712AA0B25D

**Respuesta hash crackeado 2:** mar8ia

**Hash Encontrado 3:** 5DF5D06DDC1913B052C124B5796E5741

**Respuesta hash crackeado 3:** megatron8M+

**Hash Encontrado 4:** 2faab50573cc59de5ccb7d72be270eb0

**Respuesta hash crackeado 4:** OPTi44\*-

**Documentación del reto:** cada uno de los hash se analizaron con la herramienta en kali llamada hash-identifiery con <https://gchq.github.io/CyberChef/> opción Analyse hash para obtener los tipos de hash para crackearlos:

**Hash 1:** f99452d280d7310e26ba2362cfc62ae2f090a7b1

- Para este hash se observó la pista que indicaba que el string contenía minúsculas y números, para crackearlo correctamente se utilizó hashcat por bruteforce incremental (desde 4 caracteres hasta 10 máximo) y con un juego de caracteres personalizados de solo minúsculas y números (el hash se encontraba en el archivo hash.txt).

Tipo: SHA1

comando: hashcat -m 100 -w 3 -a 3 -D 2 --increment --increment-min 4 --increment-max 10 --custom-charset1 '?l?d' hash.txt ?1?1?1?1?1?1?1?1?1

**Hash 2:** 810F91EBBD575F21C07C60B1866D6BE309503388366DECD165D74A712AA0B25D

- Para este hash no se observó ninguna pista para crackearlo correctamente se utilizó hashcat por bruteforce incremental (desde 4 caracteres hasta 14 máximo) y con todos los caracteres disponibles (el hash se encontraba en el archivo hash.txt).

Tipo: SHA-256

comando: hashcat -m 1400 -w 3 -a 3 -D 2 --increment --increment-min 4 --increment-max 14 hash.txt

**Hash 3:** 5DF5D06DDC1913B052C124B5796E5741

- Para este hash se observó la pista que indicaba que el string tenía como prefijo megatron seguido de 3 caracteres, para crackearlo correctamente se utilizó hashcat por bruteforce con el



prefijo y los últimos 3 caracteres asignados por medio de una máscara de todos los caracteres disponibles.

Tipo: MD5

comando: hashcat -m 0 -a 3 -D 2 5DF5D06DDC1913B052C124B5796E5741 megatron?a?a?a

**Hash 4:** 2faab50573cc59de5ccb7d72be270eb0

- Para este hash se observó la pista que indicaba que el string estaba compuesto de dos mayúsculas, dos minúsculas, dos números y dos caracteres especiales, para crackearlo correctamente se utilizó hashcat por bruteforce con una máscara indicando el tipo de combinaciones a realizar dada por la pista.

Tipo: MD5

comando: hashcat -m 0 -a 3 -D 2 2faab50573cc59de5ccb7d72be270eb0 ?u?u?!?!?d?d?s?s

### **Solucionario:** Reto Informático numero 17

**Respuestas:** van2021DAME, norman2021NORMAN, tierra2021TIERRA

**Enunciado:** Se tiene un volcado de memoria RAM, el cual es resultante de una investigación forense digital, y hace parte de una prueba forense. Respecto a este dump (volcado de memoria) se debe de obtener lo siguiente:

(El volcado de memoria está localizado en la carpeta reto 17 y se llama: memdump.mem)

Se deben de extraer los hashes de la SAM database que se encuentran en el volcado de memoria, y proceder a crackearlos (Solo crackear los hash de los usuarios oscorp , jean.clau de y juanes)

**Usuario 1:** juanes

**Hash SAM Encontrado 1:**

juanes:1005:aad3b435b51404eeaad3b435b51404ee:54d5ed205882ecfc551d68b1c2ab3fa0:::

**NTHash Encontrado 1:** 54d5ed205882ecfc551d68b1c2ab3fa0

**Respuesta hash crackeado 1:** tierra2021TIERRA

**Usuario 2:** oscorp

**Hash SAM Encontrado 2:**

oscorp:1006:aad3b435b51404eeaad3b435b51404ee:341963933ecd3f7eb820da843ce57635:::

**NTHash Encontrado 2:** 341963933ecd3f7eb820da843ce57635

**Respuesta hash crackeado 2:** norman2021NORMAN

**Usuario 3:** jean.clau de

**Hash SAM Encontrado 3:**

jean.clau de:1009:aad3b435b51404eeaad3b435b51404ee:141cc94ef8fe0c74c0bec1ae41bd3f41:::

**NTHash Encontrado 3:** 141cc94ef8fe0c74c0bec1ae41bd3f41

**Respuesta hash crackeado 3:** van2021DAME

**Documentación del reto:** se analizó el perfil de la imagen con la herramienta volatility detectando Win7SP1x86\_23418, Win7SP0x86, Win7SP1x86 (Windows 7 SP0/1 x86) con el comando:

volatility imageinfo -f memdump.mem

- Se Identifico la dirección virtual del archivo SAM donde se guardan las contraseñas y el registro de información SYSTEM de la maquina con el comando:

```
volatility --profile=Win7SP1x86_23418 -f memdump.mem hivelist
```

- Se obtuvieron las siguientes direcciones:

MACHINE SYSTEM

Virtual Address: 0x8901c008

Physical Address: 0x27bee008

SAM

Virtual Address: 0x899379c8

Physical Address: 0x2283a9c8

- Se volcaron los datos del archivo SAM con la dirección virtual del registro SYSTEM y el archivo SAM especificados con los parámetros -y y -s en el siguiente comando:

```
volatility hashdump --profile=Win7SP1x86_23418 -f memdump.mem -y 0x8901c008 -s 0x899379c8 > hash_SAM.txt
```

- Se copiaron los NTHash de los 3 usuarios (oscorp, jean.claude y juanes) en un nuevo archivo llamado hash.txt

- Se generó un nuevo diccionario realizando combinaciones con el archivo diccionario.txt dado y usando la herramienta princeprocessor redirigiendo la salida a un nuevo archivo:

```
pp64 --elem-cnt-min=1 --elem-cnt-max=8 diccionario.txt > newDiccionario.txt
```

- Con el nuevo diccionario generado se procede a crackear los hashes indicado la opción NTLM en la herramienta hashcat:

```
hashcat -a 0 -m 1000 -w 3 -D 1 hash.txt newDiccionario.txt
```

Las contraseñas obtenidas fueron van2021DAME, norman2021NORMAN y tierra2021TIERRA

### **Solucionario:** Reto Informático numero 18

**Respuestas:** keKkeKKeKKeKkEkEk

**Texto en el fichero felicidades.txt:** Excelente has solucionado otro reto para obtener el camino a la certificación CODSP

**Enunciado:** Se tiene un archivo de texto llamado code-decode.txt. Proceder a validar que tipo de información contiene, y luego decodificarla.

**Documentación del reto:** se creó un script en php para extraer el contenido de archivo de texto, decodificar el base64 (se identificó por los símbolos al final del texto) y guardar el contenido en un fichero png (se identificó la imagen por los bits de inicio).

```
$fileStr = file_get_contents("code-decode.txt");  
$imageDecode = base64_decode($fileStr);
```

```
file_put_contents("img_decode.png", $imageDecode);
```

El texto observado en la imagen es keKkeKKeKKeKkEkEk que seria la contraseña para descomprimir el archivo felicidades.rar

### **Solucionario: Reto Informático numero 19**

**Respuestas:** 7R1n17yN30

**Enunciado:** Se tiene un archivo llamado data. Lo que debes de hacer es identificar el tipo de archivo es, y además extraer datos (Análisis básico de binarios y de metadatos) de este archivo

**Documentación del reto:** se identificó el tipo de archivo al abrirlo con el editor hexadecimal WinHex y observar los primeros bits, al comenzar con MZ se identificó como un ejecutable de Windows, luego se utilizó la herramienta strings.exe para observar las cadenas del ejecutable y gracias a la pista que indicaba al usuario guest se filtro el texto obteniendo como respuesta la cadena guest:7R1n17yN30