Icono

Descripción generada automáticamente

Tabla de contenido

[Ejercicio 1 3](#_Toc148474908)

[Ejercicio 2 3](#_Toc148474909)

[Retos cripto 4](#_Toc148474910)

[Básico 4](#_Toc148474911)

[Cifrado por sustitución 6](#_Toc148474912)

[Codificaciones 6](#_Toc148474913)

[Avanzados 7](#_Toc148474914)

[Avanzados ll 10](#_Toc148474915)

# Ejercicio 1

***Buscar y analizar dos ataques importantes que hayan sido realizados durante los años 2022-2023. Uno de ellos debe haber tenido por objetivo el sabotaje, espionaje o fines monetarios, y otro el despliegue de ransomware. En ambos casos se deberá analizar mediante fuentes técnicas y confiables la forma de actuación, impacto y como se resolvió el incidente.***

Sabotaje a la red eléctrica de Ucrania en 2022

En febrero de 2022, antes del comienzo de la invasión de Ucrania por parte de Rusia, un ciberataque consiguió sabotear la red eléctrica de Ucrania, provocando apagones en varias zonas del país. El ataque fue reivindicado por el grupo Killnet.

El ataque se llevo a cabo mediante un DDoS (denegación de servicio distribuido), que consiste en saturar un servidor o red son solicitudes para sobrecargarlos y hacerlos inaccesibles. Los atacantes usaron botnets, es decir, redes de ordenadores infectados que de pueden controlar de forma remota.

El impacto fue considerable, ya que los apagones afectaron a servicios públicos, provocando pérdidas económicas.

El ataque fue resuelto por el gobierno ucraniano, logrando restaurar el servicio eléctrico.

Ataque de randsomware a Colonial Pipeline en 2021

En mayo del 2021, el oleoducto Colonial Pipeline, que se encarga de suministrar combustible a la costa este de Estados Unidos, fue atacado por el randsomware “DarkSide”. Esto provocó el cierre del oleoducto durante varios días, provocando escasez de combustible y aumento de los precios del combustible.

Se llevó a cabo mediante un exploit de día cero, que se uso para instalar el randsomware en sus sistemas informáticos.

El ataque fue resulto por Colonial Pipeline, que pago un rescate de 4,4 millones de dólares a los atacantes.

# Ejercicio 2

***Buscar información sobre las acciones y programas de espionaje de la NSA. Analizar las técnicas, procedimientos y colaboraciones realizadas de forma breve, y posteriormente, analizar dos proyectos a elección del alumno que se encuentren dentro del catálogo ANT TAO de la NSA, destacando los detalles de los mismos.***

El catálogo ANT TAO de la NSA contiene una lista de proyectos de tecnología de ataque. Estos se usan para desarrollar nuevas técnicas y herramientas de espionaje.

Proyect Barnacle

Se utiliza para desarrollar malware que puede infiltrarse en otros sistemas para recopilar datos, controlar sistemas o realizar ataques.

Proyect QUANTUM

Se centra en el desarrollo de técnicas de ataque que son difíciles de detectar, pudiéndose usar para espiar otros sistemas sin ser detectados. Incluye el uso de técnicas de cifrado, ingeniería social y evasiones

# Retos cripto

## Básico

Imagen que contiene Pizarra

Descripción generada automáticamenteEl alumno deberá obtener la clave para 'abrir' la caja.

Diagrama

Descripción generada automáticamente

9 23 14 14 18 5 (código proporcionado)

I W N N R E (código obtenido por sustitución)

0 1 0 1 0 1 (grupos de dos para hacer la transposición)

1 0 1 0 1 0 (código obtenido por transposicion)

W I N N E R (sustitución ordenada tras la transposision)

## Cifrado por sustitución

Obtener el texto la clave y el texto en claro para el siguiente texto cifrado:

FRZDUGV GLH PDQB WLPHV EHIRUH WKHLU GHDWKV; WKH YDOLDQW QHYHU WDVWH RI GHDWK

EXW RQFH.

Z. VKDNHVSHDUH, MXOLXV FDHVDU

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

COWARDS DIE MANY TIMES BEFORE THEIR DEATHS; THE VALIANT NEVER TASTE OF DEATH

BUT ONCE.

W. SHAKESPEARE, JULIUS CAESAR

## Codificaciones

El alumno deberá obtener el texto en claro para las siguientes codificaciones:

ZXN0byBlcyB1bmEgcHJ1ZWJhIGRlIGNyaXB0bwo=

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

esto es una prueba de cripto

NjUgNzMgNzQgNmYgMjAgNjUgNzMgMjAgNzUgNmUgNjEgMjAgNzAgNzIgNzUgNjUgNjIgNjEgMjAgNjQgNjUgMjAgNjMgNzIgNjkgNzAgNzQgNmYgMGE=

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

65 73 74 6f 20 65 73 20 75 6e 61 20 70 72 75 65 62 61 20 64 65 20 63 72 69 70 74 6f 0a

Rectángulo

Descripción generada automáticamente con confianza baja

esto es una prueba de cripto

## Avanzados

El alumno deberá descifrar los siguientes ejercicios, debiendo obtener la flag en formato "RS{flag}"

**Ejercicio 1** (¿Sabemos las dos primeras letras?):

23[M/0TW%.T9?3)8?AR%.T?%N/UGH]

Rotacion de 32

RS{mOPtwENtY\_SIX\_arENt\_EnOugh}

**Ejercicio 2** (¿XOR?):

a1a088c08b90c28680c285c0acc381ac80c39ec0879bc29d948e

a1 a0 88 c0 8b 90 c2 86 80 c2 85 c0 ac c3 81 ac 80 c3 9e c0 87 9b c2 9d 94 8e

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

01100001 00110001 00100000 01100001 00110000 00100000 00111000 00111000 00100000 01100011 00110000 00100000 00111000 01100010 00100000 00111001 00110000 00100000 01100011 00110010 00100000 00111000 00110110 00100000 00111000 00110000 00100000 01100011 00110010 00100000 00111000 00110101 00100000 01100011 00110000 00100000 01100001 01100011 00100000 01100011 00110011 00100000 00111000 00110001 00100000 01100001 01100011 00100000 00111000 00110000 00100000 01100011 00110011 00100000 00111001 01100101 00100000 01100011 00110000 00100000 00111000 00110111 00100000 00111001 01100010 00100000 01100011 00110010 00100000 00111001 01100100 00100000 00111001 00110100 00100000 00111000 01100101

**Ejercicio 3** (¿Metadatos?):

MDEwMDAxMDAgMDExMDAxMDEgMDExMTAwMTEgMDExMDAwMTEgMDExMDAwMDEgMDExMTAwMTAgMDExMDAxMTEgMDExMDAwMDEgMDAxMDAwMDAgMDExMDExMDAgMDExMDAwMDEgMDAxMDAwMDAgMDExMDEwMDEgMDExMDExMDEgMDExMDAwMDEgMDExMDAxMTEgMDExMDAxMDEgMDExMDExMTAgMDAxMTEwMTAgMDAxMDAwMDAgMDExMDEwMDAgMDExMTAxMDAgMDExMTAxMDAgMDExMTAwMDAgMDExMTAwMTEgMDAxMTEwMTAgMDAxMDExMTEgMDAxMDExMTEgMDExMDExMDEgMDExMDEwMDEgMDExMTAwMTAgMDExMDExMTEgMDAxMDExMTAgMDExMDExMDEgMDExMDAxMDEgMDExMDAxMDAgMDExMDEwMDEgMDExMTAxMDEgMDExMDExMDEgMDAxMDExMTAgMDExMDAwMTEgMDExMDExMTEgMDExMDExMDEgMDAxMDExMTEgMDExMDExMDEgMDExMDAwMDEgMDExMTEwMDAgMDAxMDExMTEgMDAxMTAxMTEgMDAxMTAwMTAgMDAxMTAwMDAgMDAxMDExMTEgMDAxMTAwMDEgMDAxMDEwMTAgMDAxMTEwMDEgMDExMTAwMDAgMDEwMDAwMDEgMDEwMDEwMTEgMDExMDAwMDEgMDEwMDAwMDEgMDAxMTAwMTAgMDAxMTAwMDEgMDExMTAxMDAgMDExMDExMTEgMDEwMTAxMDAgMDExMDEwMTAgMDExMDExMDEgMDExMDAwMDEgMDAxMTAxMTAgMDEwMTAwMDEgMDEwMTAxMTAgMDExMDEwMTEgMDEwMTEwMDEgMDEwMTAwMDAgMDExMDExMTEgMDEwMDAwMDEgMDAxMDExMTAgMDExMDEwMTAgMDExMTAwMDAgMDExMDAxMDEgMDExMDAxMTE=

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

01000100 01100101 01110011 01100011 01100001 01110010 01100111 01100001 00100000 01101100 01100001 00100000 01101001 01101101 01100001 01100111 01100101 01101110 00111010 00100000 01101000 01110100 01110100 01110000 01110011 00111010 00101111 00101111 01101101 01101001 01110010 01101111 00101110 01101101 01100101 01100100 01101001 01110101 01101101 00101110 01100011 01101111 01101101 00101111 01101101 01100001 01111000 00101111 00110111 00110010 00110000 00101111 00110001 00101010 00111001 01110000 01000001 01001011 01100001 01000001 00110010 00110001 01110100 01101111 01010100 01101010 01101101 01100001 00110110 01010001 01010110 01101011 01011001 01010000 01101111 01000001 00101110 01101010 01110000 01100101 01100111

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

Descarga la imagen: https://miro.medium.com/max/720/1\*9pAKaA21toTjma6QVkYPoA.jpeg

Un perro con la boca abierta

Descripción generada automáticamente con confianza media

**Ejercicio 4**:

.-.---......---.....-.---.....---...-.---...-..---.....---...-.---...--.---.....--.----....--.---....----...----...----....---....-.---...-.---......---.....--.----.....---......---.....--.----...-.----....---...-.-----.....--.----.....-.---...------....-.---.....--.----...-.-.---....-.---...-.-----....--.---...----...---

Texto

Descripción generada automáticamente con confianza media

.-. ---... ... ---... ..-. ---... .. ---... -. ---... -.. ---... .. ---... -. ---... --. ---... ..--.- ---... .--. ---... .- ---... - ---... - ---... . ---... .-. ---... -. ---... ... ---... ..--.- ---... .. ---... ... ---... ..--.- ---... -.- ---... . ---... -.-- ---... ..--.- ---... ..-. ---... --- ---... .-. ---... ..--. ----... -.-. ---... .-. ---... -.-- ---... .--. ---... ----... ---

R:S:F:I:N:D:I:N:G:\_:P:A:T:T:E:R:N:S:\_:I:S:\_:K:E:Y:\_:F:O:R:C:R:Y:P:O

## Avanzados ll

Se muestran a continuación los diferentes ejercicios planteados. Todos tendrán una flag del tipo "picoCTF{xxxxx}"

**Ejercicio 1**: Take each number mod37 and map it to the following character set: 0-25 is the alphabet (uppercase), 26-35 are the decimal digits, and 36 is an underscore

54 211 168 309 262 110 272 73 54 137 131 383 188 332 39 396 370 182 328 327 366 70

17 26 20 13 3 36 13 36 17 26 20 13 3 36 2 26 0 34 32 31 33 33

A: 0

B: 1

C: 2

D: 3

E: 4

F: 5

G: 6

H: 7

I: 8

J: 9

K: 10

L: 11

M: 12

N: 13

O: 14

P: 15

Q: 16

R: 17

S: 18

T: 19

U: 20

V: 21

W: 22

X: 23

Y: 24

Z: 25

0: 26

1: 27

2: 28

3: 29

4: 30

5: 31

6: 32

7: 33

8: 34

9: 35

\_: 36

R 0 U N D \_ N \_ R 0 U N D \_ C 0 A 8 6 5 7 7

**Ejercicio 2**: Se adjunta el archivo que deberá ser descifrado/decodificado.

**W H 4 7 H 4 7 H 9 0 D W 2 0 U 9 H 7**

**Ejercicio 3**: ¿Rail Fence?

Ta \_7N6DE7hlg:W3D\_H3C31N\_\_BD4ef sHR053F38N43D47 i33\_\_\_NC

Interfaz de usuario gráfica

Descripción generada automáticamente

The flag is: WH3R3\_D035\_7H3\_F3NC3\_8361N\_4ND\_3ND\_EB4C7D74

**Ejercicio 4**: Una palabra puede dar la clave...

UHQKRNWLFIYJBTODCZVAXEGSMPuhqkrnwlfiyjbtodczvaxegsmp

Lrzrxdot Jrwzutk uzovr, gfal u wzuer utk vauarjm ufz, utk hzoxwla br alr hrrajr

nzob u wjuvv quvr ft glfql fa guv rtqjovrk. Fa guv u hruxafnxj vquzuhurxv, utk, ua

alua afbr, xtytogt ao tuaxzujfvav—on qoxzvr u wzrua dzfpr ft u vqfrtafnfq dofta

on efrg. Alrzr grzr ago zoxtk hjuqy vdoav truz otr rsazrbfam on alr huqy, utk u

jotw otr truz alr oalrz. Alr vqujrv grzr rsqrrkftwjm luzk utk wjovvm, gfal ujj alr

uddruzutqr on hxztfvlrk wojk. Alr grfwla on alr ftvrqa guv erzm zrbuzyuhjr, utk,

auyftw ujj alftwv ftao qotvfkrzuafot, F qoxjk luzkjm hjubr Ixdfarz noz lfv odftfot

zrvdrqaftw fa.

Alr njuw fv: dfqoQAN{5XH5717X710T\_3E0JX710T\_7H755H1U}

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Hereupon Legrand arose, with a grave and stately air, and brought me the beetle

from a glass case in which it was enclosed. It was a beautiful scarabaeus, and, at

that time, unknown to naturalists—of course a great prize in a scientific point

of view. There were two round black spots near one extremity of the back, and a

long one near the other. The scales were exceedingly hard and glossy, with all the

appearance of burnished gold. The weight of the insect was very remarkable, and,

taking all things into consideration, I could hardly blame Jupiter for his opinion

respecting it.

The flag is: picoCTF{5UB5717U710N\_3V0LU710N\_7B755B1A}

**Ejercicio 5**: ¿Una transposicion manual que tal?

heTfl g as iicpCTo{7F4NRP051N5\_16\_35P3X51N3\_VC85A020}E

Agrupamos los caracteres por grupos de 3, contando los espacios como un carácter mas.

La transposition seria de 012 a 201, quedandonos la siguiente frase.

The flag is picoCTF{7R4N5P051N6\_15\_3XP3N51V3\_5C82A0E0}

**Ejercicio 6**: Se ha identificado que la clave del mensaje cifrado es "CYLAB" y que se debe usar un algoritmo que comienza por "V"...

rgnoDVD{O0NU\_WQ3\_G1G3O3T3\_A1AH3S\_a23a13a5}

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente con confianza media

picoCTF{D0NT\_US3\_V1G3N3R3\_C1PH3R\_y23c13p5}