



#HackTheQuestion

trc



/Rooted® CON

1.- ¿Sabrías decirme cuál es el mensaje escondido?

VEIUSVRPL1RPVEkvVEIUT1RJVEkKVEIUT1RPVE9UTy9UT1RPVE9UT1RPCIRJVE9UT
1RJL1RPVEIUT1RPL1RPVEkvVEIUSVRPVEkvVEIUT1RJL1RJVEIUT1RJCIRPVE9USVR
PL1RJVE9USQpUT1RJVE9USS9USVRPVEkvVEkvVEIUSVRPVEkvVE9USVRJVEkvVEI
UTy9UT1RJL1RJVEIUT1RJL1RPVE9USVRJVE9UTwpUT1RJVE9UTy9UT1RJL1RJVEIUT
1RJCIRPVEIUS9USVRJVEIUS9USVRPVEkKVEIUSVRPVEkvVE9USS9UT1RPVE8vV
EIUT1RJL1RJVE8KVE9UT1RPL1RJVEIUSVRPL1RJVE8vVE9USS9USS9USVRJVEIUTy9
UT1RJVEIUSQpUSVRPVEIUSQpUT1RJVE9UTy9UT1RJL1RJVEIUT1RJCIRPVEIUS9U
SVRJVEIUS9USVRPVEkKVEIUTy9UT1RJVEIUSQ==

- a) La ciberseguridad es una inversión, no un centro de coste
- b) Hay 10 clases de personas, las que entienden binario y las que no
- c) El software es como el gas, se expande hasta que llena el espacio que lo contiene
- d) Trata tu contraseña como a tu cepillo de dientes: no dejes que nadie más la use y cámbiala cada seis meses.

2.- Si consigues descifrar esa imagen, podrás averiguar el último libro que me he comprado y que estoy deseoso de leer:

- a) Linux de cero a ninja, de @CiberPoliES
- b) Tecnologías de ciberseguridad, de Rafa López
- c) Historias cortas sobre fondo azul, de Willy Obispo
- d) Gestión de Incidentes de Seguridad, de Maite Moreno



3.- De vez en cuando me tomo un Dry Martini en casa, pero no uno cualquiera. Hay varias recetas y distintos sabores según el toque personal. ¿quieres saber el mío? (pssss: he ocultado mí truco - **en la foto del enlace, aquí no** - utilizando el método de copia binaria)

- a) Mezclado, no agitado.
- b) Martini Fiero con 30 ml de Ginebra
- c) Vesper Martini con 30 ml de Vodka
- d) Hielo Classic picado



4.- Te pasas horas y horas concienciando a tus usuarios, explicando cómo debe ser una password y la importancia de proteger las credenciales. Casi todos ellos te entienden y te hacen caso, pero tampoco falta el que no le importa un pepino.

¿Sabes con quien voy a tener una pequeña charla?

- a) Eva: 947c111729f048b54f99f9ea55414a85fdf055e9fc2a281dcbcd318b47daddf8
- b) Alfredo:
06b2600adfce49290b4e199e557512b7890f25cebe03eb3a10ea0e2834996fec
- c) Marta:
266b5e2f62625ca6e7ab507dbdf48de3cc8e1002551a729eec383311dcdaa10f
- d) Javi:
6ca13d52ca70c883e0f0bb101e425a89e8624de51db2d2392593af6a84118090

5.- Desde hace años perseguimos a un peligroso ciber criminal que se hace llamar Woody Kalamidad y que hasta ahora no había dejado huella alguna, pero finalmente hemos averiguado su correo (**k4lam1dad@gmail.com**) y gracias a ello ahora sabemos un lugar que frecuenta y le vamos a detener. ¿sabes dónde montaremos la trampa?

Esta vez deberéis escribir la respuesta en modo CTF, es decir
Flag{esto_es_un_ejemplo}

Respuesta: Flag{XXX}

6.- Hoy hemos celebrado una sesión preparatoria de nuestro Kick-off anual, donde nos han dado un esbozo de lo que serán las líneas estratégicas de la empresa para este año. Lo hemos hecho en un sitio agradable. ¿sabrías decirme dónde?

Nuevamente deberéis escribir la respuesta en modo CTF, es decir
Flag{esto_es_un_ejemplo}



Respuesta:

Flag{XXX}

7.- Las Fuerzas y Cuerpos de Seguridad del Estado han interceptado un correo entre narcotraficantes, pasándose información. El correo tiene anexo un fichero jpg con un plano, que indica el lugar donde está escondido el alijo. No han sido capaces de averiguarlo y nos piden ayuda con urgencia porque es necesario encontrar el lugar antes de que distribuyan la mercancía. ¿Pistas? solo hay una referencia escrita en el correo: '*La X marca el lugar*'. Nada más. Menuda estupidez.



- a) Doniños
- b) Brión
- c) Seixo
- d) Xubia

8.- Quizá no lo sabéis o simplemente no os habéis fijado, pero el logo del Cibercomando Militar de EEUU (el US CYBER-COM) contiene un código secreto incluido en el anillo dorado central y lógicamente tiene su propio significado. El código es un hash calculado a partir de un string ¿Serías capaz de averiguar la cadena de texto que origina ese hash?



- a) "If you can read this, send your resume to jobs@nsa.gov"
- b) "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."
- c) "Loyalty and Constancy - Cleverness and Dexterity"
- d) "This is our code: As the nation's first line of defense in cyberspace, we operate at the speed, relevance, and scale necessary to win."

9.- Me han pasado este fichero pcap para analizar. Quieren que busque quien se ha conectado al servidor, porque la está liando. Necesito encontrar el usuario y su password. Please, help!!

- a) User: fake Password: user
- b) User: admin Password: admin
- c) User: user Password: abc123
- d) User: admin Password: 123456

10.- Echarme una mano. No soy capaz de leer el contenido de este fichero. Nada es lo que parece 😊

- a) La mayoría de las APT, en realidad, no son muy avanzadas
- b) A tu adversario no le importa que tu sysadmin se haya ido hace 10 años
- c) La salida de una ciber crisis solo es el comienzo de la siguiente
- d) Tu adversario no esperará a que termines de parchear

11.- Tenemos un incidente de ciberseguridad que hemos calificado de crítico y nos vendría bien conocer la atribución para adelantarnos a su próximo movimiento.

Y el caso es que hay alguien que nos está ayudando de manera anónima y nos está dando pistas, pero no, tiene que ser un enigma, ¿qué le costaba darlas en claro?

- a) APT28
- b) APT29
- c) Sandworm
- d) Turla

12.- Llevo siguiéndolo unos días. Su comportamiento ha cambiado. No me fio un pelo de él. Se esconde y llama desde el móvil y no sé con quién. Seguro que nos está vendiendo. Pero esta vez lo tengo. No he podido entender la conversación, pero he podido grabar mientras marcaba y voy a descubrir a quien llama.

- a) Embajada Americana
- b) Embajada China
- c) Embajada Rusa
- d) Delegación de Hacienda

13.- Dentro de la cifra clásico, este es sin duda mi sistema preferido. El inventor me parece un genio: el primer método de cifrado polialfabético. No te será difícil encontrar qué nombre lleva este método (aunque realmente, él no es el autor original) lo que te llevará a descifrar el mensaje. La clave es simple.

Yzmcoik zqhfplipdd ww kacdmvcqc nsf xqffiñga qhqywzldd

46

A	a	b	c	d	e	f	g	h	i	l
B	m	n	o	p	q	r	s	t	u	x
C	a	b	c	d	e	f	g	h	i	l
D	x	m	n	o	p	q	r	s	t	u
E	a	b	c	d	e	f	g	h	i	l
F	u	x	m	n	o	p	q	r	s	t
G	a	b	c	d	e	f	g	h	i	l
H	t	u	x	m	n	o	p	q	r	s
I	a	b	c	d	e	f	g	h	i	l
L	s	t	u	x	m	n	o	p	q	r
M	a	b	c	d	e	f	g	h	i	l
N	r	s	t	u	x	m	n	o	p	q
O	a	b	c	d	e	f	g	h	i	l
P	q	r	s	t	u	x	m	n	o	p
Q	a	b	c	d	e	f	g	h	i	l
R	p	q	r	s	t	u	x	m	n	o
S	a	b	c	d	e	f	g	h	i	l
T	o	p	q	r	s	t	u	x	m	n
V	a	b	c	d	e	f	g	h	i	l
X	n	o	p	q	r	s	t	u	x	m

M ij

- a) Quien no tiene metas, es poco probable que las alcance.
- b) Sun Tzu dice: el arte de la guerra se basa en el engaño.
- c) **Grandes resultados se consiguen con pequeños esfuerzos.**
- d) Tienes que creer en ti mismo y todo se andará entonces.

14.- Nuestro cliente ha recibido una extorsión por un supuesto delito que no ha cometido, y fruto de los nervios ha pagado el rescate solicitado (más de 2K\$) en este wallet: 3BRYJKJCsNJ5ayRxFsnwrAeKARcVNsojUq

Ahora estamos rastreando las transacciones efectuadas después del pago y queremos saber el ID de la cuenta a la que han ido a parar 0.01714147 BTC. ¿puedes ayudarme?

- a) 3QKDh-b4nvR
- b) 37F2i-qA6oP
- c) bc1q3-czgya
- d) 34C1e-ycWmG

15.- Hoy empieza /RootedCON y me he currado esta camiseta para ir al evento. Si no la entiendes es porque se te escapa algún concepto de criptografía simétrica y lo peor es que no podrás resolver este reto. Si lo has pillado, aun tendrás que averiguar otra cosa para descifrar este mensaje:

MzEwZTU5NTExZDA4MDYxOTBhNTIxNjUzMDQ0ZTQzMGMQwYzQ5MDAwNDE4
MDA=



- a) Este concurso se acabó
- b) Hasta el año que viene
- c) Que reto más horrible!
- d) Yo quiero esa camiseta