RETOS DEL CONCURSO CTF
ProtAAPP @ RootedCON

🚩 Utiliza el **siguiente formulario** para enviar tus respuestas 🚩

RETO 1: Calentando motores

ENUNCIADO

Queremos que RootedCON 2026 tenga mucho éxito.Empezamos suave con un reto sencillo. Mira a ver si puedes descifrar este código.

Q2FsZW50YW5kbyBtb3RvcmVzIHBhcmEgUm9vdGVkQ09OLiBObyBoZSBwdWVkZSBwZXJkZXIgZWwgdHJhY2sgZGUgUHJvdEFBUFAgZWwgdmllcm5lcyA2IGRlIG1hcnpvLiBUZW5kcmVtb3MgZXhjZWxlbnRlcyBwb25lbnRlcyB5IG9zIGhlbW9zIHByZXBhcmFkbyBtaWxlcyBkZSBzb3JwcmVzYXMuIFkgc2kgdG9kbyBzYWxlIG1hbCwgeWEgc2FiZXMgIGN1bHBhIGVzIGRlIFdpbGx5LiBUZSBlc3BlcmFtb3Mu

Y ya sabes, para contestar tienes que obtener el hash MD5 de la solución e incluirla en la respuesta de esta manera: flag{HashMD5delaSolución}

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 2: El Menú

ENUNCIADO

¿Qué se come aquí? Me da que este QR con el menú de RootedCON no tiene una lista muy larga de tapas y pinchos para comer en Kinépolis

Fichero adjunto: QRmenu-Reto02.png
URL: Reto 2

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 3: Un DNS curioso

ENUNCIADO

Hmmm, ¿has visto los registros DNS del dominio ttx.es? ¡Qué extraño!
¿Es posible que uno de ellos tenga un mensaje oculto?

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 4: La paleta de colores

ENUNCIADO

Esta imagen parece una paleta de colores para decorar una fiesta gótica, pero la realidad es que esconde un mensaje.

Fichero adjunto: paleta_colores.png
URL: Reto 4

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 5: Tiempo para leer

ENUNCIADO

Jo, me han recomendado este libro, pero lo cierto es que no puedo abrirlo. Debe estar corrupto o algo así. ¿alguien que lo pueda abrir?

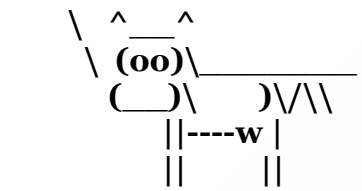
Fichero adjunto: LookAtMe.pdf
URL: Reto 5

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 6: La vaca loca

_____

< ENUNCIADO >



Me he instalado el programa CowSay en Linux, que es una herramienta que muestra una vaca (y otros animales) junto con un mensaje en forma de pensamiento. Pero ahora va la vaca esta y me dice no sé qué ...

"OOOMoOMoOMoOMoOMoOM ..." (ver charla completa de la vaca en fichero adjunto)

¿Tú la entiendes?

Fichero adjunto: Muuuuu.txt
URL: Reto 6

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 7: Hierros

ENUNCIADO

Si te gusta la mecánica, la ingeniería y sobre todo la seguridad, te gustarán estos cacharros antiguos que demuestran que hace cientos de años ya tenían tanta imaginación como nosotros ahora o más.

Si adivinas lo que muestra esta foto y dónde la he tomado, no te costará mucho trabajo saber a quién se lo compró.

Fichero adjunto: Hierros.jpeg
URL: Reto 7

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 8: Estrenamos nueva web

ENUNCIADO

Hemos remodelado la web de ProtAAPP, pero como andamos flojos de pasta se la hemos encargado a uno que tenía pinta de cuñao. Yo no sé si hemos hecho bien, por que este tipo, de seguridad, ... igual no.

¿Alguien puede comprobar si es posible hacer un bypass del login?

Os paso la URL de la web: https://protaapp.github.io/RootedCON26-reto8/

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 9: ¿Culpable o Inocente?

ENUNCIADO

- ➔ Juez: ¿Cómo se declara el acusado de los cargos que se le imputan?
- ➔ Willy: Inocente, Señoría.

  Yo no pude cometer el crimen que me imputan, cometido la mañana del 1 de septiembre de 2025 a las 10:00 horas, porque en ese mismo momento estaba haciendo login en mi estación de trabajo, a más de 60 Km de la escena del crimen.

  Y para demostrarlo, le adjunto el log de eventos de seguridad del directorio activo y de la consola de los EDR que así lo demuestran
- ➔ Juez: Fiscal, envíe los ficheros a analizar por un perito forense y en una semana emitiré mi resolución.

¿Qué veredicto dictaminará el juez? ¿"INOCENTE" o "CULPABLE"?

El motivo de tu sentencia es importante, ¡no olvides dejarla en los comentarios!

Ficheros adjuntos: SecurityEventLog.txt y LogEDR.json
URL: Reto 9

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 10: Suspicious email

ENUNCIADO

Equipo,

Os paso un correo reportado como phishing con malware.

Adjunto la captura relacionada para que investiguéis el incidente.
El cliente de correo no consigue abrir el adjunto correctamente. Revisad el mensaje en bruto y extraed manualmente la evidencia.

Ya me diréis cuál era el malware que se intentaba colar

Ficheros adjuntos: suspicious-email.eml
URL: Reto10

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 11: Usa la cabeza

ENUNCIADO

La cabeza de caballo es solo un detalle de un magnífico monumento diseñado como homenaje a un escritor.

Si consigues localizar la ciudad donde se encuentra, no te será difícil averiguar el nombre del evento internacional que se ha celebrado allí hace unos días y que tiene mucho que ver con la ciberseguridad

Ficheros adjuntos: escultura.jpg
URL: Reto 11

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 12: Check your Software

ENUNCIADO

Los más viejos se acordarán.

Hace muuuuchos años, una institución europea creó un 'virus', que no era un virus, sino algo inocuo con el que probar que tu antivirus estaba bien instalado. Eso ya no sirve de mucho. Actualmente los motores antivirus lo miran por encima del hombro, ven que no entraña peligro y no se molestan en alertar (solo quedan 2 antivirus despistados en Virus Total que hacen saltar las alarmas).

Pero la idea era buena. Tanto, que se inventó lo mismo para el correo no solicitado ¿sabes que hay que añadir a tu correo para poder probar tu filtro anti-spam?

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 13: Tres ratones ciegos

ENUNCIADO

Un asesino anda suelto.

La policía ya tiene perfilado su modo de operar (sus TTPs). Está reproduciendo los libros de la escritora Agatha Christie uno a uno y, si es fiel a la fecha de publicación, esta vez le toca imitar a los asesinatos de la novela 'TRES RATONES CIEGOS', donde atrapará a un grupo de personas en un espacio desconocido y los irá aniquilando.
Se cree tan listo y está tan convencido de su plan, que no le importa dar pistas. Ha mandado un mensaje a los inspectores que llevan el caso: un audio que puede resolver el reto e indicar el lugar del crimen.

Queda poco tiempo para descubrir la ubicación donde se producirá el siniestro y si no lo encontramos a tiempo, aquello acabará siendo una ratonera.

Ficheros adjuntos: TresRatonesCiegos.wav
URL: Reto13

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 14: Art ATT&CK

ENUNCIADO

Para resolver este reto no hace falta que te rompas la cabeza, pero sí tendrás que ser ordenado y poner cada cosa en su sitio.

Ficheros adjuntos: File01.txt, File02.txt, File03.txt, File04.txt, File05.txt, File06.txt
URL: Reto 14

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

RETO 15: El archivo que no debería existir

ENUNCIADO

Deja que te cuente una historia corta, que tiene un fondo... perverso.

Durante las últimas semanas, hemos recibido en el buzón info@protaapp.com correos de muchos integrantes de la asociación -quizá alguno tuyo-, así como de organizaciones afines o simpatizantes, historias sobre un patrón de ataque cuanto menos inquietante. Alguien -o algo- está dejando rastros digitales en sistemas donde jamás debería haber actividad. No son intrusiones normales. No hay logs, no hay IPs, no hay firmas. Solo... restos. Como si una presencia invisible hubiese pasado por allí, manipulando datos y borrando sus huellas con una precisión casi quirúrgica. Aunque hemos solicitado que nos enviasen evidencias, todas las respuestas en las que nos decían haber adjuntando capturas o ficheros, nos llegaban siempre vacías. Es como si los archivos se evaporasen en el éter...net.

Pero ayer, a las 03:17 una vieja placa Atmel ATMega644 que compramos por Ebay en diciembre de 2011, que nadie recuerda por qué sigue encendida, registró un único evento. Un archivo apareció en su raíz. No fue creado, no fue descargado, no fue copiado. Simplemente apareció.

El archivo no tiene extensión. No tiene metadatos. No tiene autor.

Solo un nombre: **r15**.

Fichero adjunto: r15

URL: Reto 15

¿Quieres saber algo más inquietante? La placa lleva años sin estar conectada a internet, la hemos escaneado con Flipper Zero, pero tampoco presenta actividad inalámbrica, ni tiene servicios expuestos, ni usuarios activos desde hace meses. Es, en teoría, un sistema muerto. Pero ahí está el fichero.

Con todo el jaleo de organizar el track de RootedCON no hemos podido determinar si se trata de un fichero de naturaleza maliciosa. No parece contener malware conocido, no ejecuta nada, no responde a ningún patrón típico, pero quienes lo hemos visto pensamos igual: no se trata de un archivo ordinario.

Alguien lo dejó ahí a propósito.
Alguien que sabía que acabaría en tus manos.
Tu misión es simple en apariencia: descubre qué oculta en su interior.
Dicen que algunos secretos no quieren ser encontrados.
Dicen que hay información que se protege a sí misma.
Dicen que hay puertas que, una vez abiertas, no pueden cerrarse.
Pero tú no estás aquí para escuchar advertencias.
Estás aquí para resolver el misterio.

El archivo te espera. O no, tú decides.

Respuesta: flag{HashMD5delaSolución} [Enviar respuesta]

Esperamos que os hayan gustado y os hayan resultado divertidos. Nos vemos en RootedCON en la gran final.

Correo electrónico: info@protaapp.com
Web: http://www.protaapp.com