

HACKCØN+ES+

(hackcontest)

Introducción

¿Alguna vez te has preguntado “**cómo hacen los hackers**”? ¿Cómo se meten en los sistemas o cómo consiguen saltarse las protecciones?

Si sientes curiosidad, si quieres experimentar “**qué es eso**”, si quieres comprenderlos mejor, en definitiva, si quieres aprender, **ÉSTE** es tu concurso.

¿Qué es?

HACKCØN+ES+ es un concurso de **seguridad informática** en el que sus participantes deberán enfrentarse a **distintos desafíos** y tratar de superarlos empleando distintas técnicas, el ingenio y el sentido común.

HACKCØN+ES+ es una competición con la que **todo el mundo** puede aprender y divertirse, ya que tiene desafíos con distintos niveles de dificultad. Todo el mundo tiene una oportunidad de sacarle partido y de hacer su aportación. No

es sólo para "expertos".

HACKCØN+ES+ tiene cómo principal objetivo el de acercar, de una forma amena y gradual, el mundo de la seguridad informática a todo el mundo, en forma de retos que nos harán ponernos en la piel de un "hacker" y así poder entender mejor cómo funcionan las cosas desde una perspectiva única: desde "el otro lado".

¿Cómo funciona?

HACKCØN+ES+ funciona como un portal web. Los participantes deberán acceder a la página principal de dicho portal y darse de alta para poder jugar, inscribiéndose con un **alias/nick** y una **dirección de correo electrónico** (válida) dónde recibirán un enlace para poder confirmar su alta.



fig.1: formulario de registro

Una vez inscritos, deberán autenticarse en el portal para poder acceder al **listado de** los distintos **desafíos** disponibles, que aparecerán indicados con su nombre, descripción y valoración (puntos otorgados por resolverlo). Desde este listado se podrá acceder a cada uno de los desafíos, dentro de los cuales se darán las instrucciones necesarias para poder realizarlo y superarlo.

Todos los **desafíos son independientes** y están disponibles desde el principio, de manera que si algún participante se atasca en uno, siempre podrá intentar otro y por tanto tendrá las mismas oportunidades que cualquiera.

HACKCØN+ES+ sólo puede tener un ganador: aquel que resuelva el mayor número de desafíos (itodos si es posible!) antes que nadie. Existe un "ranking" público en el que todo el mundo (participante o no) puede ver cómo evolucionan la competición y los competidores: quién va en cabeza, cuantos puntos tiene, que pruebas ha resuelto y en qué orden.

HACKCØN+ES+ es automático y gana quien acaba primero en el ranking. Aún así, toda la actividad del concurso es registrada y existe un responsable del concurso que puede exigir datos adicionales, explicaciones, etc. y que también hará de juez para dirimir cualquier conflicto que surja durante el desarrollo de la competición.

Desafíos

HACKCØN+ES+ incluye multitud de desafíos, de toda clase y dificultad, en los que se puede requerir conocimientos específicos o simplemente algo de ingenio, y, en todo caso, sentido común. Los desafíos son independientes, y pueden ser pruebas que se realicen directamente en el portal (por ejemplo un formulario web que hay que superar), pruebas que requieran la descarga de algún fichero (un ejecutable, un texto, una imagen...) o incluso pruebas que requieran el acceso a otros sistemas (wifi, ssh, servidores web, sockets, MVs, etc.).



The screenshot shows a web browser window with the URL `http://hackcontest.tenerife-lanparty.com:666/?op=desafios`. The page title is "TENERIFE 2k9 | hack contest" and the sub-header is "| desafíos |". On the left, there is a terminal window showing the output of a program, with "hACKCØN+ES+" at the top. On the right, there is a table listing 10 challenges with their IDs, names, descriptions, and values.

id	nombre	descripción	valor
1	desafio_01	Supera este sencillo formulario	4
2	desafio_02	Otro formulario sencillo	5
3	desafio_03	Uno de base de datos SQL	10
4	desafio_04	Un formulario un tanto enrevesado.	20
5	desafio_05	Un formulario muy especial...	15
6	desafio_06	Hackea la wifi del concurso	20
7	desafio_07	Criptografía: ¿cual es la frase secreta?	15
8	desafio_08	necesitarás un linux	20
9	desafio_09	Una imagen vale más que...	10
10	desafio_10	nivel de criptografía	10

Below the table, there is an "AVISO: El concurso finaliza a las 17:00." and a note: "necesitas pistas? quieres preguntar algo? entra en el canal [#Tenerife-HC](#) del [irc-hispano.org](#)". At the bottom, there are links for "inicio" and "ranking".

fig.2: listado de desafíos

Actualmente **HACKCØN+ES+** cuenta ya con desafíos que abarcan campos tan variados como la esteganografía, la criptografía, bases de datos (múltiples variedades), depuración/desensamblado, sistemas de autenticación débil, depuración de comunicaciones, etc. etc. pruebas tanto para entornos gnu-linux como windows.

HACKCØN+ES+ tiene además una peculiaridad, cualquiera puede desarrollar desafíos para el sistema, es parte de la competición: si a algún participante se le ocurre un nuevo desafío, puede desarrollarlo utilizando el SDK que incluye el sistema. Una vez incorporado este desafío en el concurso el participante que lo ha creado ya tiene una prueba más en su haber (iya sabe cómo resolverla!), mientras que el resto deberán superarla. De esta manera se fomenta que la

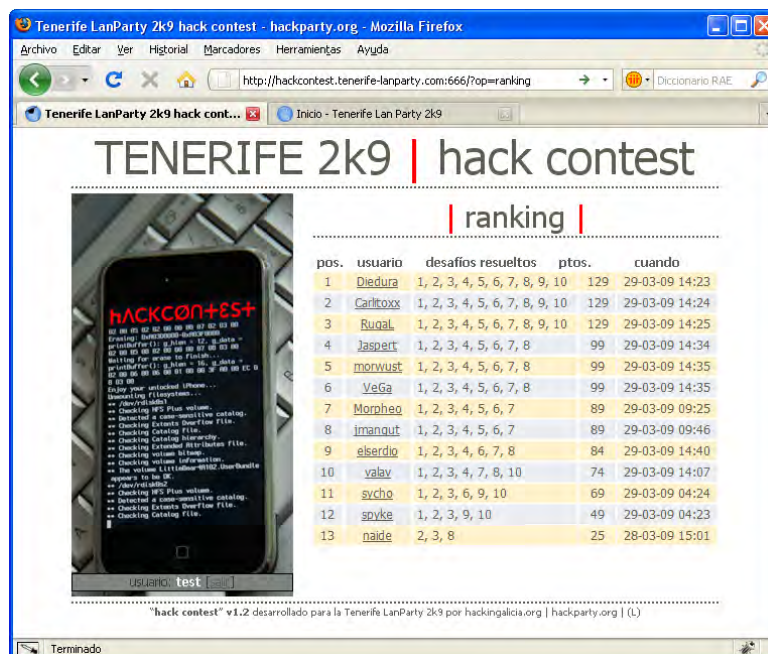
gente se involucre más activamente, ya que los demás participantes se verán impulsados a realizar sus propios desafíos para competir en igualdad de condiciones. Cuanto mayor la calidad de la prueba, mayor puntuación y mayor beneficio. Es un sistema retroalimentado.

Dinámica

hACKCØN+ES+ es un sistema que se puede arrancar o detener a voluntad. Cuando la organización lo decida, se pone en marcha y comienza su andadura. A partir de ese momento los participantes se pueden apuntar y comenzar a competir inmediatamente.

hACKCØN+ES+ es una competición participativa, en la que se fomenta el intercambio de información con la organización, pero también entre participantes. Normalmente se acompañará de algún sistema que permita **"dialogar"** a los competidores, como puede ser un foro, un chat IRC, un servidor jabber, etc. (la organización decidirá el método más conveniente). A través de este medio se resolverán dudas (que siempre surgen!!), se responderán preguntas y, si es necesario, se darán pistas, de manera que el concurso resulte dinámico y entretenido.

hACKCØN+ES+ cuenta con un ranking público, donde TODO el mundo (participantes o no) podrán comprobar en tiempo real cómo evoluciona la competición: cómo se adelantan, cómo son superados, las pugnas por cada puesto, las carreras, quien ha resuelto primero esta prueba o aquella, etc... ies como seguir cualquier otro deporte!



pos.	usuario	desafios resueltos	ptos.	cuando
1	Diedura	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	129	29-03-09 14:23
2	Carltoxx	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	129	29-03-09 14:24
3	Ruqal	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	129	29-03-09 14:25
4	Jaspert	1, 2, 3, 4, 5, 6, 7, 8	99	29-03-09 14:34
5	monvust	1, 2, 3, 4, 5, 6, 7, 8	99	29-03-09 14:35
6	VeGa	1, 2, 3, 4, 5, 6, 7, 8	99	29-03-09 14:35
7	Morpheo	1, 2, 3, 4, 5, 6, 7	89	29-03-09 09:25
8	imanqui	1, 2, 3, 4, 5, 6, 7	89	29-03-09 09:46
9	alserdie	1, 2, 3, 4, 6, 7, 8	84	29-03-09 14:40
10	valav	1, 2, 3, 4, 7, 8, 10	74	29-03-09 14:07
11	sycho	1, 2, 3, 6, 9, 10	69	29-03-09 04:24
12	svyke	1, 2, 3, 9, 10	49	29-03-09 04:23
13	naide	2, 3, 8	25	28-03-09 15:01

fig.3: Rankig de participantes/pruebas

hACKCØN+ES+ se ha pensado para que la gente aprenda y se divierta mientras lo hace, por eso en muchas ocasiones (decisión de la organización) se realiza durante su desarrollo (o previamente a su comienzo) un taller en el que

se da una pequeña introducción a algunas técnicas, a diversas herramientas y en general se dan ideas sobre cómo afrontar este tipo de retos.

Normas

hACKCØN+ES+ se rige por una máxima general: **"CASI TODO VALE"**. Aún así la competición está regularizada, para que los límites queden establecidos. Estas son las **"normas oficiales"**:

- Para participar en el concurso es necesario inscribirse.
- No está permitido causar daños al sistema de competición (eso no quita que se le busque las cosquillas... :)
- No está permitido causar daños a los contrincantes (eso no quita que también se les busquen las cosquillas... ;))
- Los participantes podrán ser individuos o grupos, pero no ambas cosas a la vez, esto es, **no se permitirá que los integrantes de un grupo se apunten individualmente y participen conjuntamente.**
- Normalmente no es necesaria la fuerza bruta para resolver ninguna de las pruebas, aunque si pueden ser necesarios ataques repetitivos.
- Cada participante deberá documentar la resolución de las pruebas, ya que dichas explicaciones podrán ser solicitadas por la organización (por cualquier razón y en cualquier momento).
- El incumplimiento de cualquiera de estas normas puede ser motivo de expulsión de la competición.
- La organización del concurso tiene la última palabra en cualquier decisión acerca de la competición :)

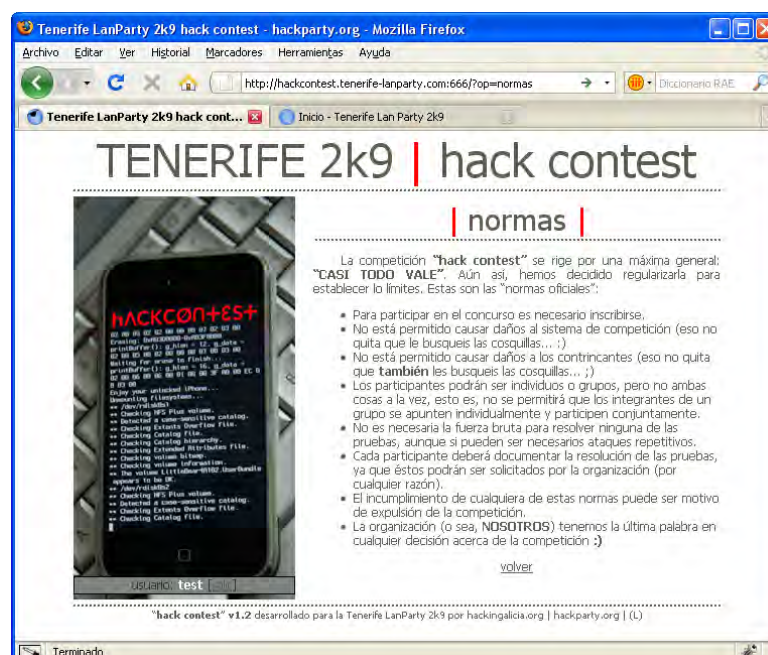


fig.4: Normas de la competición

El sentido común es lo que debe regir en casos o situaciones dudosas. El espíritu de la prueba es el de aprender, el de divertirse, el de experimentar..

Buscar los límites es lícito (e incluso aplaudido), pero nunca nunca hagas daño al entorno o a tu contrincante de manera perniciosa: espía, copia, sonsaca, investiga... pero no borres datos, alteres cuentas o equipos, o en general causes perniciosa.

Requisitos

hardware:

- un servidor limpio que se pueda instalar desde 0 (tiempo estimado 2 horas: instalación y puesta en marcha)
- conexión a la red del evento, con una tarjeta de red rápida (se recomienda tarjeta de red Gigabit, aunque depende del volumen de participantes/tráfico y de la red)

software:

- acceso a Internet desde el servidor (necesario para las actualizaciones, envío de correos de alta, etc.)
- una dirección IP fija para el servidor y una dirección IP fija para cada una de las MVs (máquinas virtuales) que se utilicen en el concurso (se usarán MVs o no en función de los desafíos)
- ACCESO ILIMITADO a los puertos del servidor y de las MVs (sin restricciones de cortafuegos o sistemas de control).
- OPCIONALMENTE: recomendamos que se pueda acceder a las máquinas del concurso mediante un nombre (p.ej. <http://hack.dominio-int.es/>), es decir, que haya resolución DNS para las IPs asignadas.

para los participantes:

- acceso al servidor/MVs del concurso desde la red (a ser posible mediante el nombre)
- acceso a Internet para la búsqueda de herramientas, documentación, pistas, etc. y para la parte de participación pública (IRC, jabber, IM, etc.)