Publicado en la revista @rroba, nº 68, pp. 16-19. Mayo, 2003. 

# Hack21: diario de un participante

## 2ª Edición del concurso de hacking ético

**Ha pasado más de un año desde la celebración de lo que fue un concurso pionero en España. Con unos meses de retraso, Hack21 se ha presentado de nuevo a la Comunidad y una vez más, allí hemos estado, participando, cara a cara con otros compañeros y concursantes. Desde la posición privilegiada que nos ha brindado este hecho, narraremos escrupulosamente todo lo acontecido durante la celebración del concurso. También contaremos con la opinión de la otra cara de la moneda: los organizadores del evento.**

### Un poco de historia

A finales de Octubre de 2001 se inauguraba oficialmente el primer concurso de hacking ético celebrado en España; su nombre, Hack21. En aquella ocasión el concurso resultó empañado por diversos motivos, como la extrema dificultad o una mala planificación del mismo, lo que propició que los participantes pasaran la mayor parte de su tiempo atacando un formulario infranqueable, cuando la vulnerabilidad que se debía explotar estaba en otra parte (concretamente en el servidor DNS). Para más inri, la máquina del concurso ejecutaba un sistema operativo poco corriente para la mayoría de los participantes lo que dificultaba la confección del exploit necesario para superar el primer nivel del concurso, y además el concursante debía tener acceso a un dominio, para que la explotación del fallo DNS fuera posible. Por último, se intentó arreglar el desaguisado a última hora y a la desesperada, añadiendo una nueva vulnerabilidad, en uno de los servicios RPC de la máquina.

Este último intento también fue en vano, ya que el servicio RPC caía cada dos por tres, debido a los intentos de explotación por parte de los concursantes. Como resultado, el premio se declaró desierto y la verdad, no quedó muy buen sabor de boca entre el público al que iba destinado el evento, que se sintió de alguna forma estafado y defraudado.

### La nueva edición

El concurso de este año ha durado algo menos de un mes. Comenzó el 4 de Febrero a las 14:00h (con unas horas de retraso, hora española) y finalizó el viernes 28 de Febrero a las 14h. Se dividía en tres niveles de dificultad creciente y a cada uno de ellos correspondía un premio (una misma persona podía resultar ganadora de los tres premios ya que sólo se premiaba al primer concursante que superara cada uno de los niveles, de forma independiente). Los premios eran muy atractivos: una cámara digital, 1500 € y 3000 €, para los niveles 1, 2 y 3, respectivamente. Además, en los tres casos se haría entrega de un trofeo, y para los 100 primeros se regalaría también una suscripción a una revista de seguridad. En realidad, el concurso estaba diseñado para que la probabilidad de que alguien ganara el premio correspondiente al último nivel fuera ínfima, con lo cual lo de los 3000 € era más una maniobra de marketing que otra cosa.


## El nivel 1

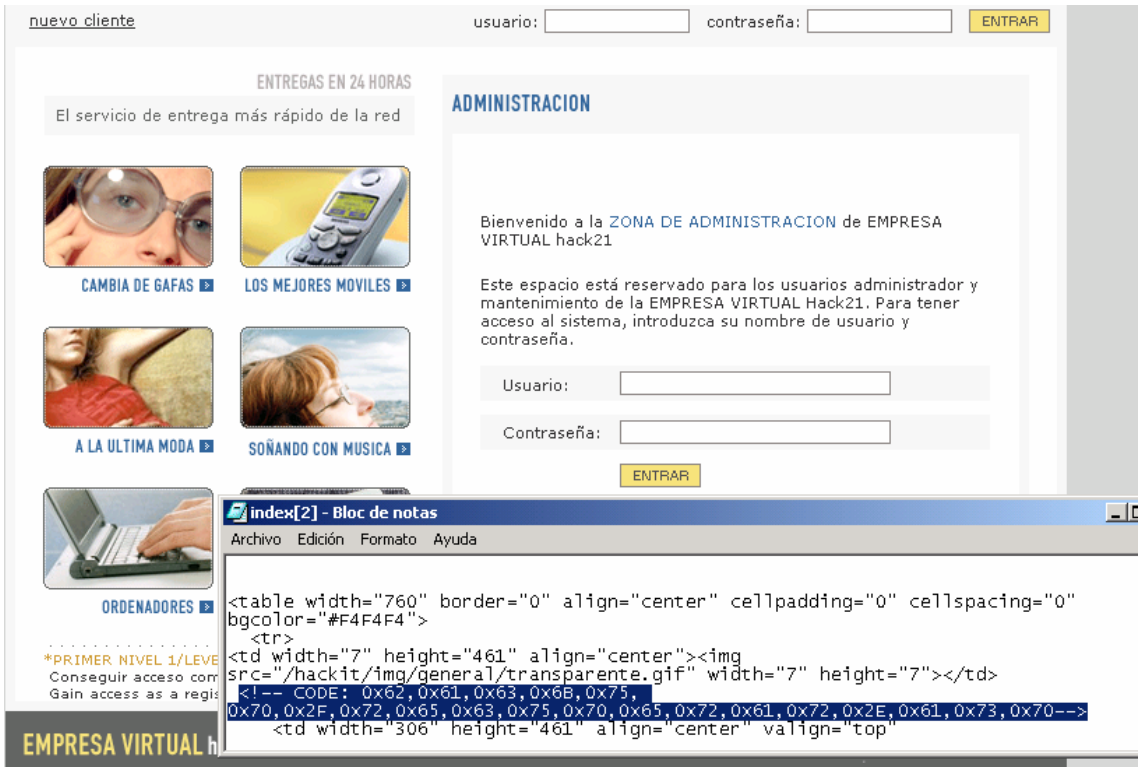
Todos los niveles se basaban en una aplicación (en ASP) creada a efectos del concurso y que emulaba una tienda de comercio electrónico. La plataforma empleada era Windows 2000 / IIS 5.0 / SQL Server 2000 (lógico, si tenemos en cuenta que Microsoft era uno de los patrocinadores del concurso). Existían dos páginas: la propia del concurso (hackit.hack21.com) donde se desarrollaban las pruebas, y otra (www.hack21.com) donde se encontraban las reglas del concurso, descripción de los premios y dos foros: uno destinado a los propios concursantes y otro para noticias oficiales de la organización.

Nada más conectar a la página web del concurso teníamos acceso al catálogo de productos de la tienda virtual, con fotos, descripciones y precios. Arriba a la derecha se podía ver un formulario para entrar en la tienda como usuario registrado, mediante usuario y contraseña. Precisamente éste era el objetivo del primer nivel: conseguir acceder a la tienda como un usuario registrado. Evidentemente no había formulario de registro gratuito sino una interfaz de administración, al que inicialmente no se tenía acceso: “no está en el rango de clase permitido, sólo acceso desde la LAN y/o no tiene acceso”. Para saltarnos esto, simplemente había que modificar la cookie y sustituir dos variables por los valores adecuados. La cookie quedaba así: “src=172%2E16%2E16%2E1; permiso=1; ASPSESSIONIDSQTQDTQQ=…”. Para averiguar la clase de la dirección a IP a usar, bastaba con hacer telnet al puerto 80 del servidor web e introducir “HEAD / HTTP/1.0”, lo que le provocaba la visualización de la IP privada del servidor web y nos daba una idea sobre el direccionamiento usado.

Por fín estábamos ante el formulario de administración pero ¿conocíamos el usuario y contraseña de la persona encargada de esta función? El usuario se podía intuir

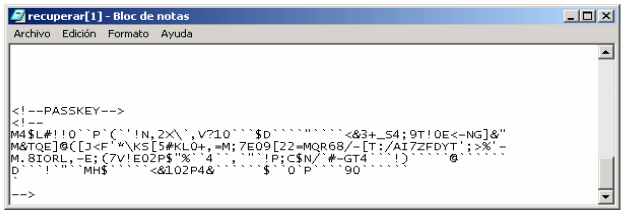
de otro mensaje de error, puesto a propósito, que decía: “el administrador y el usuario de mantenimiento son los únicos que pueden dar de alta usuarios nuevos”. Dicho error se mostraba al intentar acceder al enlace “nuevo usuario”, el cual no valía para nada más. ¿Y la contraseña? Bastaba con analizar el código HTML de la página para encontrar:

<!-- CODE: 0x62,0x61,0x63,0x6B,0x75,0x70,0x2F,0x72,0x65,0x63,0x75, 0x70,0x65,0x72,0x61,0x72,0x2E,0x61,0x73,0x70-->. Traduciendo el comentario HTML a texto quedaba: “backup/recuperar.asp”. Así llegábamos a una nueva página, con el dibujo de una llave y aparentemente nada más. Pero si nos fijábamos otra vez en el código HTML de la página, abajo del todo, teníamos un fichero codificado con “uuencode”. Bastaba con decodificarlo para obtener así un archivo ZIP. Dentro del mismo, se encontraba un segundo fichero, el cual no se podía extraer de buenas a primeras, al estar protegido por contraseña. Había pues que crackear el archivo ZIP. Este punto ha sido duramente criticado, por un lado debido a la obvia dependencia de esta prueba con la CPU de que disponga cada concursante, lo que introduce desigualdades entre los mismos; y por otro, porque la contraseña del ZIP resultó tener 8 caracteres, lo cual significaba días (sí, días) de tiempo de cracking para poder romperla, usando un charset normal (números y letras mayúsculas-minúsculas), incluso en una máquina potente (pongamos, 1-2 GHz). Consiguieron romper la contraseña un grupo de concursantes que optaron por distribuirse el espacio de claves posibles, lanzando así un ataque distribuido. La contraseña resultó ser: “opqlmoeh”. Evidentemente, si hubiésemos sabido de antemano que la contraseña no incluía mayúsculas ni números, el proceso de fuerza bruta se habría visto tremendamente reducido. Pero no contábamos con esa información.




El fichero extraído contenía los hashes (LanMan y NT) correspondiente al usuario cuyo id era el 1010. Tras adecuar el fichero al formato correcto aceptado por la

conocida herramienta L0pthcrack, comenzábamos una nueva fase de fuerza bruta. En algo más de 5h teníamos la contraseña: "vutiZUviGi" (a pesar de la longitud de la contraseña, este tipo de hashes se pueden romper fácilmente debido a la naturaleza débil de los mismos; más información en el manual de L0pthcrack). Era de suponer que el id 1010 se correspondía con el usuario de administración. Sólo restaba dirigirse al formulario de administración e introducir como usuario "mantenimiento" junto con la contraseña anteriormente hallada. Habíamos superado el nivel y debíamos rellenar un pequeño formulario con los datos reales del concursante, para que la entrega de premios fuera factible. Estos datos privados (que incluían usuario, contraseña, nombre y apellidos, dirección postal completa y e-mail) serían más adelante comprometidos, debido a una mala securización por parte de S21sec. Este grave hecho ha dado mucho que hablar. Suerte que nadie lo denunció a la APD… En cualquier caso, añadir que el ganador de este nivel fue un inteligente concursante apodado "Dreyer".




**El nivel 2**

Al contrario que el nivel 1, este nuevo nivel se podía resolver fácilmente y en su totalidad, en cuestión de horas. Lo más lógico es que igualmente lo hubiera ganado "Dreyer", precisamente por contar con la ventaja de haber llegado el primero. No fue así, hubo irregularidades que lo impidieron, anulando injustamente esta ventaja. ¿Cuáles? No seáis impacientes, todo a su debido tiempo.

Comenzamos a jugar en este nivel horas más tarde de que Dreyer lo hiciera. El objetivo era realizar una compra de un producto determinado de la tienda, pero claro, nuestro usuario registrado no contaba con saldo suficiente. Había un formulario de búsqueda sospechoso, pero que no funcionaba: obteníamos un error de VBScript extraño y sobre el que nada se podía hacer. Pasamos unos dos días estudiando y analizando todo el escenario y nada, que no había manera. Hablamos con otros concursantes y estaban en la misma situación. Ya cansados, uno de ellos preguntó en el foro de S21sec si dicho formulario funcionaba correctamente. Si no recuerdo mal, hubo que insistir una vez más hasta que los organizadores repasaran el script .asp del formulario de búsqueda y descubrieran que no funcionaba. ¡Estaba mal programado! Y para colmo, ¡era la única puerta al siguiente nivel! ¡Habíamos tirado por la borda dos bonitos días! S21sec se disculpó del tremendo fallo y cerró el nivel hasta las 10h del día siguiente. No salíamos de nuestro asombro pues era temprano, principio de la tarde.

¿Tanto se tarda en arreglar un .asp? Mientras tanto, y durante esos más de dos días de incertidumbre, el pánico cundió en los foros, publicaron incluso la solución al nivel 1, y hubo bastante gente que llegó al nivel 2 de una manera injusta. Ahora comprendéis lo de las irregularidades a las que me he referido antes.


Son las 10h del día siguiente. El nivel 2 comienza a funcionar, con el .asp de búsqueda operativo (por fin). El que más tarde resultaría ganador de este nivel y que había superado el nivel 1 la tarde de antes, "Mandingo", está ahí puntual. Según pudimos saber a posteriori, sobre las 13h aproximadamente ya había superado el nivel, aunque la organización no lo notificaría oficialmente hasta media tarde. No tuvimos siquiera oportunidad porque por motivos personales no pudimos empezar a jugar hasta aproximadamente media mañana. Por aquel entonces, Mandingo ya era ganador o estaba a punto de serlo. Aunque no perdimos el tiempo: aparte de superar el nivel en unas horas, y sin ser el siguiente nuestro objetivo, acabamos descubriendo cosas interesantes…

El nivel 2 se superaba mediante inyección SQL a través del recién arreglado formulario de búsqueda. Simplemente había que inyectar: ';exec dt_setcash_u 'romansoft','hack21'--. Ya está, este nivel era más sencillo que el primero, y muchísimo menos costoso en términos de tiempo. Sólo había que indagar un poco en las tablas de sistema del SQL Server, no había que ser ningún experto en SQL Server; bastaba con utilizar Google y los documentos sobre "injecting" de NGSSoftware. Como paso previo, tuvimos que inyectar: kkkk' union select 1,'a',1,text,1 from syscomments--. Esto nos muestra la tabla "syscomments", dentro de la cual se definía el "store procedure" que debíamos utilizar para pasar de nivel (dt_setcash_u):

CREATE PROC dt_setcash_u @usuario varchar(10), @pass varchar(7) AS if (@pass ='hack21') UPDATE cliente SET saldo = 3000 WHERE usuario = @usuario. Al ejecutar el procedimiento, y si la contraseña era la correcta, nuestro saldo se actualizaba a 3000, que era justo la cantidad necesaria para poder comprar el producto y superar el nivel. Una solución completamente artificial y distante de la realidad.

También mediante inyección era posible obtener acceso a la tabla que guardaba los datos privados que los concursantes habían rellenado al superar el nivel 1. Notificamos inmediatamente a S21sec, quien nos requirió pruebas. Se las dimos, y al rato, el servidor del concurso era misteriosamente desconectado, sin ningún tipo de aviso. La mayoría de la gente nunca supo la verdadera razón, nosotros sí. Entre medias, el login de usuarios al nivel 2 dejó de funcionar (los organizadores habían cambiado los permisos sobre la tabla en cuestión, causando un mal funcionamiento generalizado de la aplicación). Al rato, el servidor volvió a ser activado y de nuevo investigamos la vulnerabilidad descubierta. Esta vez, S21sec había cambiado de estrategia: no había cerrado completamente el agujero sino que lo había parcheado. El formulario usado para inyectar filtraba ahora, mediante una expresión regular, la cadena correspondiente al nombre de la tabla en cuestión. Se pretendía evitar así la manipulación de la misma. Nos reímos bastante, porque una vez más era trivial obtener acceso a la tabla: bastó con cambiar algunas mayúsculas a minúsculas (o viceversa), de forma que nos saltamos el filtro, sin alterar la sentencia SQL usada (parece que S21sec ignoraba que SQL Server es case-insensitive). Notificamos la vulnerabilidad por segunda vez a S21sec, y esta vez exigimos que eliminaran nuestros datos personales de dicha tabla, visto que eran incapaces de protegerlos adecuadamente.

**El nivel 3**

Simplemente era infranqueable. Consistía en añadir una cierta cadena de texto (en realidad, un hash MD5 que identificaba al concursante) a la página principal de la tienda virtual. Para ello, era necesario hackear el sistema, ya fuera a través del propio servidor web o bien del servidor de bases de datos. Teniendo en cuenta que tanto el IIS 5.0 como el SQL Server 2000 estaban completamente actualizados, securizados (por ejemplo, la mayoría de objetos de IIS habían sido deshabilitados) y con los últimos parches aplicados, sin olvidar las medidas de protección adicionales (como un firewall), la prueba resultaba extremadamente difícil hasta para el hacker más experimentado del planeta. Se requería descubrir una nueva vulnerabilidad (en apenas dos semanas que restaban de concurso) en un software cerrado (no disponemos de acceso al código fuente) o hacer uso de algún exploit "0-day" (es decir, no público), si es que realmente lo hubiera. No es de extrañar pues que nadie superara este nivel y S21sec se guardara para sí los 3000 € presupuestados para el premio.

**Una buena idea pero…**

…una mala implementación. Con estas palabras podríamos resumir el concurso de este año. La historia se repite y, es una pena, porque las intenciones no creemos que hayan sido malas. Quizás S21sec debería poner más cuidado o destinar más recursos para el próximo concurso. Deseamos de todo corazón que tomen nota de nuestras críticas (siempre constructivas), y el año que viene no vuelvan a caer en los mismos errores. A

la tercera va la vencida, esperemos. Al menos, siempre nos quedará la satisfacción de haber quedado entre los seis primeros puestos.


**Entrevista a S21sec –organizadores de Hack21-**

*@rroba.-* ¿Qué les ha llevado a montar este concurso? ¿Le reporta beneficio alguno a S21sec?
*S21.-* S21sec, empresa de Seguridad Telemática Avanzada, nació en Febrero de 2000 a raíz del primer congreso de hackers que se celebró en España en Septiembre de 1999. Conociendo nuestros orígenes siempre quisimos organizar un concurso de hacking propio con la idea de reunir anualmente a todos los amantes de la seguridad para la puesta en común de todas las técnicas de seguridad y poner en práctica sus conocimientos y habilidades. S21sec, persigue con estas iniciativas concienciar a las organizaciones de los riesgos a los que se enfrentan y busca dar a conocer la importancia de las técnicas de hacking ético a la hora de securizar los sistemas de información.

*@rroba.-* ¿Cuánto tiempo les ha llevado preparar el concurso? ¿Qué infraestructura tanto técnica (servidores, ancho de banda, software, etc) como humana se ha escondido tras el mismo?
*S21.-* A mediados de Octubre del pasado año, nos pusimos en marcha en la organización de la segunda edición del Concurso Hack21, empezamos a idear las pruebas que podrían diseñarse y a obtener los patrocinios oportunos. Y, fue a finales de Diciembre cuando el equipo de desarrollo puso todos sus esfuerzos en la preparación del mismo.

*@rroba.-* ¿Qué infraestructura tanto técnica (servidores, ancho de banda, software, etc) como humana se ha escondido tras el mismo?
*S21.-* El concurso ha requerido de 5 máquinas: un servidor web, un servidor de Base de Datos, un Firewall para el concurso, un Firewall para la administración y un NIDS.

- Servidor Web, Servidor Windows 2000 Advanced Server, IIS 5.0 y HIDS
- Servidor Base de Datos, Windows 2000 Server, SQL Server 2000 y HIDS
- Firewall Concurso, Servidor Linux e Iptables
- Firewall Administración, Servidor Linux, Iptables, centralizador de logs
- NIDS y consola de Administración de los HIDS

*@rroba.-* ¿Podrían describir brevemente el proceso de securización que se ha aplicado a los servidores del concurso? ¿Han utilizado su solución HIVE?
*S21.-* Principalmente y resumiendo en el servidor de Aplicación y el Servidor de Base de Datos se aplicaron diferentes técnicas y políticas de seguridad propias de S21sec así como recomendadas por Microsoft. Los cortafuegos sólo dejaban acceso al puerto 80 y a los servicios de administración que eran únicamente accesibles por S21sec. En breve, podréis disponer de un informe completo sobre la securización del concurso en nuestra web.

Por último, HIVE, cortafuegos de aplicaciones web desarrollado por el equipo de S21sec, no estuvo presente en el concurso pero creemos que el método de encriptación empleado así como las restricciones que se establecieron en el foro han podido confundir a los participantes.

*@rroba.-* En el foro del concurso se ha hablado de un grave hecho: la fuga de datos personales debido a un mal diseño del nivel 2. ¿Qué tienen que decir al respecto?
*S21.-* Durante la implementación del concurso cometimos el error de utilizar la base de datos que contenía la vulnerabilidad necesaria para la superación del nivel 2 para almacenar detalles de los usuarios que superaban dicho nivel. Un concursante nos advirtió del problema y procedimos a solucionarlo de inmediato, eliminando los detalles de los concursantes del nivel 2 de la base de datos afectada.

*@rroba.-* También ha habido quejas respecto al primer nivel, porque su solución suponía dos pruebas de fuerza bruta, una de las cuales (obtener la contraseña de un .zip) estaba pensada para consumir abundantes recursos (ciclos de CPU) de los ordenadores de los concursantes. Dicho con otras palabras: teniendo en cuenta que no todos los concursantes tienen un ordenador potente, ¿consideran justo que un nivel tenga una tan alta dependencia de la CPU? ¿Por qué se ha diseñado así el nivel? ¿Les parece comprensible el enfado de muchos concursantes que se estancaron en la prueba de cracking, simplemente por el hecho de que no contaban con un ordenador lo suficientemente potente?
*S21.-* Las críticas de los participantes sean buenas o malas son importantes y a tener en cuenta para futuras ediciones. Realizar un concurso que guste a la mayoría puede ser factible pero será prácticamente imposible que guste a la totalidad de los concursantes.

El primer nivel (cookie, archivos) en ningún momento pretendía ser un caso real, nadie hace un filtrado de IPs con cookies. Lo que se buscaba era conseguir que todos los participantes tomasen parte en la superación de este nivel y lo logramos con creces. Eran pruebas sencillas pero requerían ciertas dosis de investigación y paciencia,

virtudes imprescindibles para cualquier persona con dedicación a la seguridad informática.
El segundo nivel (SQL Server), requería de unos conocimientos avanzados en SQL Server y SQL Injection para superar la prueba.

*@rroba.-* ¿Han considerado la posibilidad de hacerle una oferta de trabajo a alguno/s de los mejores concursantes de esta edición? ¿Qué opinan de esta posible forma de cazar talentos?
*S21.-* En esta edición hemos contado con participantes cuyos perfiles se adecuan a los demandados por S21sec por lo que dejamos la puerta abierta a esta posibilidad.

*@rroba.-* El tercer y último nivel ha consistido en encontrar alguna vulnerabilidad en software comercial tan probado y auditado como Microsoft IIS 5.0 o SQL Server 2000, con todos los últimos parches de seguridad aplicados. ¿Realmente pensaban que alguien lo lograría? ¿Cuál era la intención de una prueba así?
*S21.-* A diferencia de los 2 primeros niveles que se basaban en problemas y vulnerabilidades conocidas, el tercer nivel requería del descubrimiento de una nueva vulnerabilidad. Sabemos que no hay ningún servidor 100% seguro en Internet por lo que este nivel podía haber sido superado a través de una investigación interna, exploits "0 days" no públicos u otras fuentes.

*@rroba.-* ¿Qué conclusiones han sacado del desarrollo del concurso? ¿Cuál es el balance?
*S21.-* El resultado del concurso ha sido muy positivo y estamos francamente satisfechos. Hay cosas que mejorar para próximas ediciones pero la elevada participación y el reconocimiento obtenido nos dicen que organizaremos una tercera edición.

*@rroba.-* ¿Cuántos concursantes han participado? ¿Cuántos no españoles? ¿Cómo calificarían el nivel técnico de los mismos? ¿Y su comportamiento humano (participación en el foro, posibles ataques DoS, etc)?
*S21.-* En total se inscribieron 1600 participantes de los cuales el 80% fue de nacionalidad española y el 20% restante de países sudamericanos (Argentina, Chile, Colombia, Méjico), EEUU y Europa en su mayoría. El nivel técnico de los mismos fue muy elevado aunque únicamente 30 personas fueron capaces de superar el segundo nivel en el tiempo establecido.

*@rroba.-* ¿Cuánto tendremos que esperar para el Hack21 3ª Edición?
*S21.-* La tercera edición está prevista para dentro de 1 año.

Román Medina-Heigl Hernández
-[ RoMaNSoFt ]-
roman@rs-labs.com

[ http://www.rs-labs.com/ ]