Publicado en la revista @rroba, nº 61, pp. 16-19. Octubre, 2002.

iZhal: una comunidad dedicada al hacking
Introducción a los "wargames"

Aunque la Legislación a veces no es demasiado clara al respecto entrar en computadoras ajenas sin permiso expreso del dueño se considera delito en muchos países y está penado por la Ley. Realizar actividades relacionadas con el hacking conlleva sus riesgos. Os presentamos a continuación una forma divertida y didáctica de poner a prueba vuestros conocimientos y habilidades más oscuras sin que esto suponga en ningún momento sobrepasar la frontera de la legalidad.

Los "wargames"

"Juegos de guerra" es la traducción literal. Detrás de esta vaga traducción se esconde todo un mundo que hará las delicias de cualquier aficionado al hacking. La idea de aprender jugando no es nueva pero dada la naturaleza a veces ilegal de este arte que es el hack y la sana rivalidad que suele existir entre distintos hackers, cobra un especial interés este tipo de juegos donde la gente pueda poner a prueba su ingenio y habilidades técnicas de un modo seguro, competitivo y totalmente legal.

También se les suele llamar "challenges" (retos o desafíos, en castellano) y hay de diferentes tipos. Los más serios y difíciles (a veces imposibles) ofrecen premios de gran cuantía y en muchos casos nadie consigue resolver el reto. Suelen ser ofrecidos por empresas que quieren poner a prueba sus productos o beneficiarse de la publicidad que pueda suponer "un producto que nadie ha podido hackear o romper". Hace no mucho tiempo la empresa Meganet ofrecía todo un Ferrari al que consiguiera romper un cierto cifrado que ellos idearon y al que se referían como "encriptación de matriz virtual" ("virtual matrix encryption"); nadie consiguió romperlo aunque esto no implica la robustez del mismo (en este caso no se daban los suficientes datos como para que alguien pudiera realizar una buena labor de criptoanálisis sobre el cifrado). Antes de eso la empresa Argus Systems ofreció $50000 al que consiguiera romper la seguridad de uno de sus productos (Pitbull). En este caso el grupo LSD se llevó la palma y resultó ganador al aprovechar una vulnerabilidad en el kernel del sistema (Solaris x86).

Dentro de la modalidad anterior aunque con premios más austeros y una dificultad menor podemos encasillar a los concursos que lanzan algunas revistas del sector o los que se celebran en el seno de diferentes eventos de seguridad (por ejemplo, la llamada "toma de la bastilla" de la recién celebrada NcN party) donde el objetivo suele ser penetrar en un sistema a toda costa, y donde (casi) todo vale.

Aunque quizás sea cuestión de terminología y es algo un tanto subjetivo, a mí me gusta diferenciar entre los dos casos anteriores, y un tercer y último caso, que es a lo que denominaremos "wargame" propiamente dicho y que será el núcleo de este artículo. Estos últimos son juegos que gozan de unas ciertas características que lo diferencian de un simple concurso o de un reto como el de Argus. Para empezar, se componen de diferentes niveles (o pequeños retos) independientes pero que deben ser superados en orden secuencial (normalmente) y donde la dificultad crece a medida que aumentamos de nivel. No se permite usar fuerza bruta (salvo en pruebas cuyo objetivo es

precisamente ejercitar este tipo de técnica, como por ejemplo, al crackear un archivo de contraseñas) ni hackear el servidor que alberga el wargame; normalmente cada nivel es diseñado teniendo en mente una o varias formas bien definidas de ser superado, que son las que el participante deberá encontrar. No suele haber premios (o si los hay serán muy pequeños, incluso simbólicos) aparte de la propia satisfacción personal por haber conseguido superar las distintas pruebas y llegar hasta el final. Están enfocados a aprender; en muchos casos, la propia web del wargame ofrece tutoriales o enlaces hacia diversas fuentes que ayudarán a resolver cada una de las pruebas. También suele haber disponible uno o varios foros donde los distintos participantes pueden intercambiar ideas e incluso ayudarse unos a otros (aunque no se permite que la gente revele soluciones directas ni pistas demasiado explícitas ya que rompería la tónica del juego). Por último, suele haber tablas de clasificación ("Hall of Fame") donde podemos ver en qué nivel se encuentra cada participante o incluso la fecha en que éste supero cada uno de los niveles. Es un aliciente más el intentar ser el mejor o simplemente superar a otro amigo que esté participando en un mismo juego.

Los primeros pasos

Participar en un wargame es tan simple como rellenar un pequeño formulario de registro donde al menos se te pide un nombre de usuario, para diferenciarte del resto de compañeros, y una clave que nos autentifique convenientemente. También se suele pedir una dirección de e-mail aunque esto no es estrictamente necesario. A partir de ahí nuestra cuenta es creada y cada vez que vayamos a jugar debemos validarnos ante una ventana de login (a no ser que nuestro navegador posea alguna cookie persistente u otra funcionalidad que haga este trabajo por nosotros de forma transparente).

Dependiendo del juego una vez hecho el login estaremos ante un menú o página web que nos dará acceso a las distinas funcionalidades disponibles como el foro, consultar las tablas de clasificación o simplemente empezar a jugar en el primer nivel. En este último caso es posible que se nos muestre una pequeña información explicando el objetivo de dicho nivel o algo que nos oriente para que sepamos en qué consiste el mismo. En muchos casos no existe esta orientación y tendremos que valernos del sentido común, astucia, recurrir al código fuente de la página o simplemente fijarnos en algún detalle de la misma. No todo es técnica pura y dura; también se trata de que el participante tenga los ojos bien abiertos y sepa extraer información de donde aparentemente no la hay.

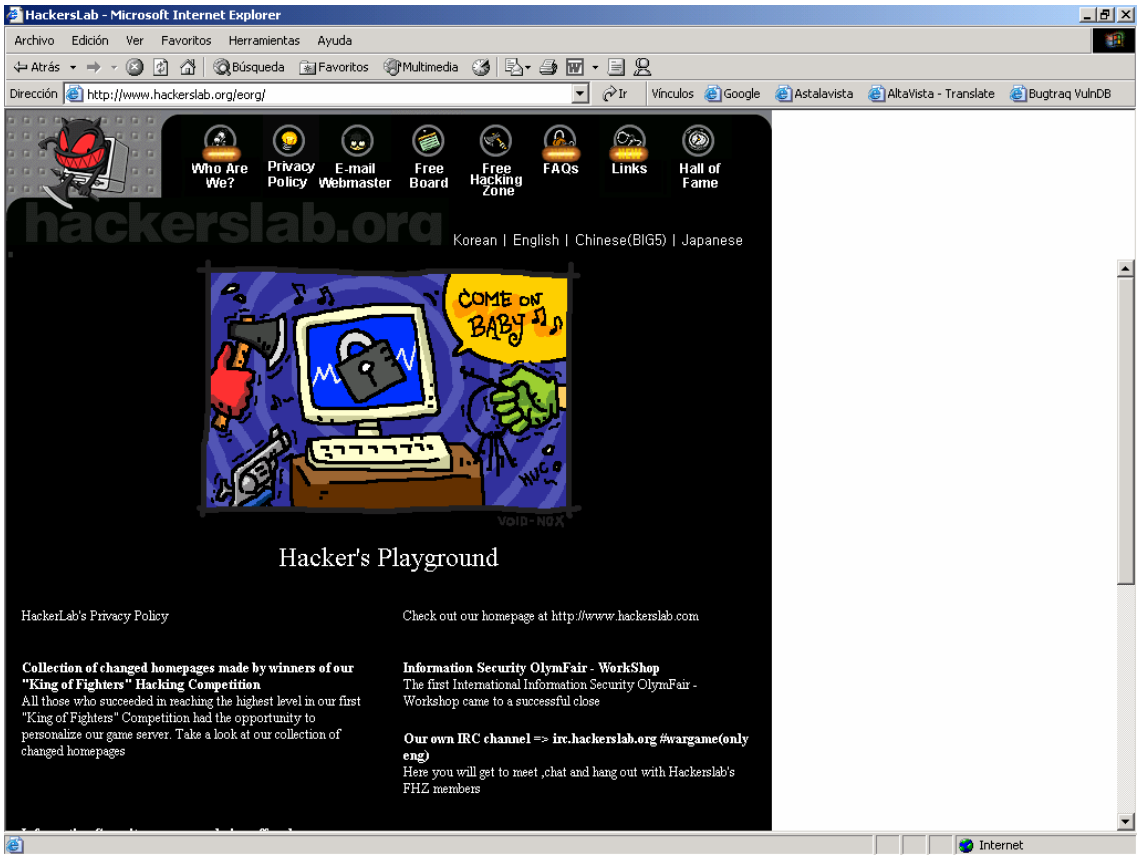
Eligiendo el wargame adecuado

Para comprender el funcionamiento de un wargame lo mejor es verlo con nuestros propios ojos y probarlo: apuntarnos a uno de ellos. Existe un gran abanico de juegos disponibles en la red, unos más sofisticados que otros, unos más famosos y conocidos, y otros que no lo son tanto. Más reales o al contrario más "fantásticos". Algunos están orientados a un sistema operativo en particular. Otros hacen hincapié en aspectos de programación, mientras que el resto son menos técnicos y más orientados al entretenimiento.

A no ser que dispongamos de todo el tiempo del mundo lo mejor es empezar apuntándose a alguno de los juegos "conocidos" dejándonos guiar por el criterio de amigos o conocidos que tengan experiencia en el tema (no hace falta que sean expertos pero al menos deben haber superado un número aceptable de niveles para tener una panorámica del juego en cuestión lo suficientemente amplia como para poder juzgar y opinar con conocimiento de causa).

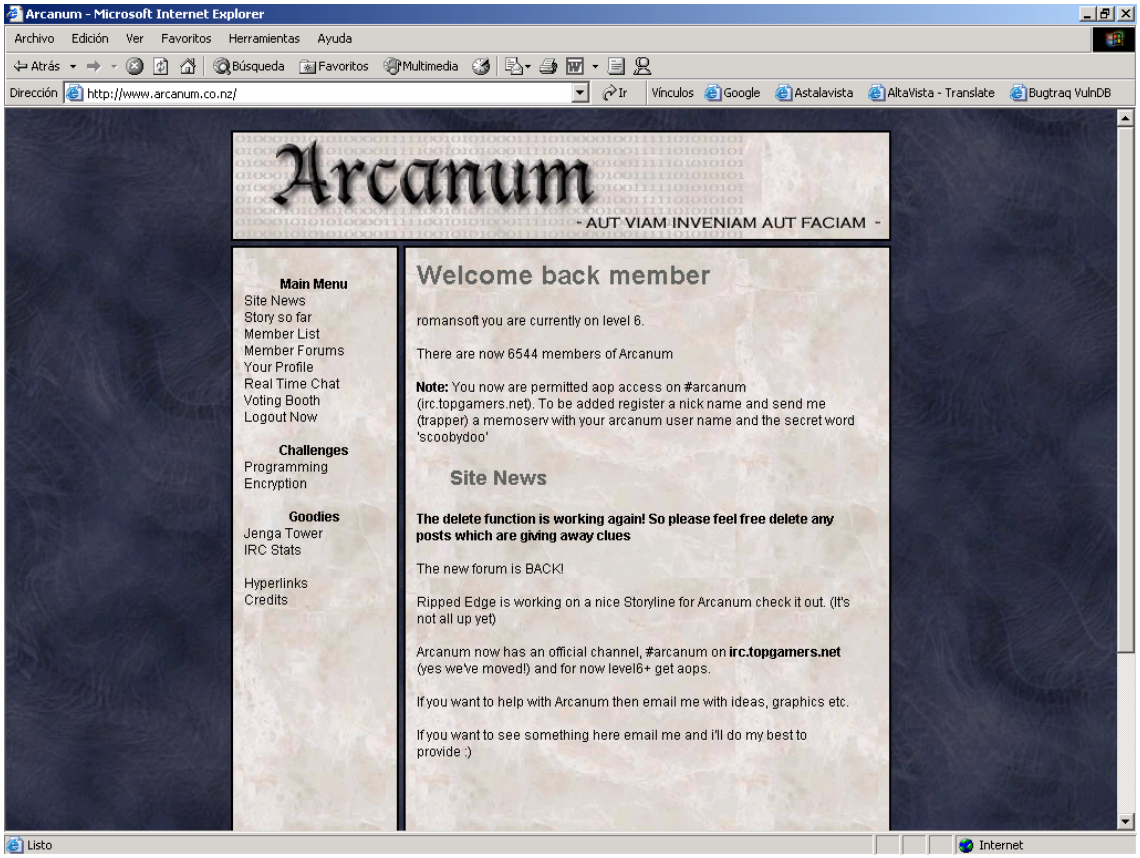
Ni mucho menos pretendemos realizar una lista exhaustiva o guía de wargames; nuestro objetivo es simplemente que podáis elegir un wargame para comenzar lo más acorde posible a vuestras preferencias y que os deje un buen sabor de boca. Sin más dilaciones pasamos a comentar brevemente algunos de los juegos en los que el autor de este artículo ha tenido la oportunidad de participar activamente:

- **Hackerslab** (http://www.hackerslab.org/eorg/): es muy técnico y está totalmente orientado al mundo Unix. Es de lo más real que he visto ya que tendréis que programar vuestros propios exploits y aplicar técnicas tan conocidas y reales (pero no por ello dejan de ser importantes) como son los típicos "stack-based buffer overflows" (desbordamiento de pila), "format string bugs" (vulnerabilidades de cadena de formato), "1-byte buffer overflow" (caso particular y peculiar de los buffer overflow) o "race condition attacks" (ataques de tipo condición de carrera), entre otros. Altamente recomendado pero quizás no apto para alguien con conocimientos nulos o muy básicos en entornos Unix. En inglés (¡con algunos textos en coreano!).

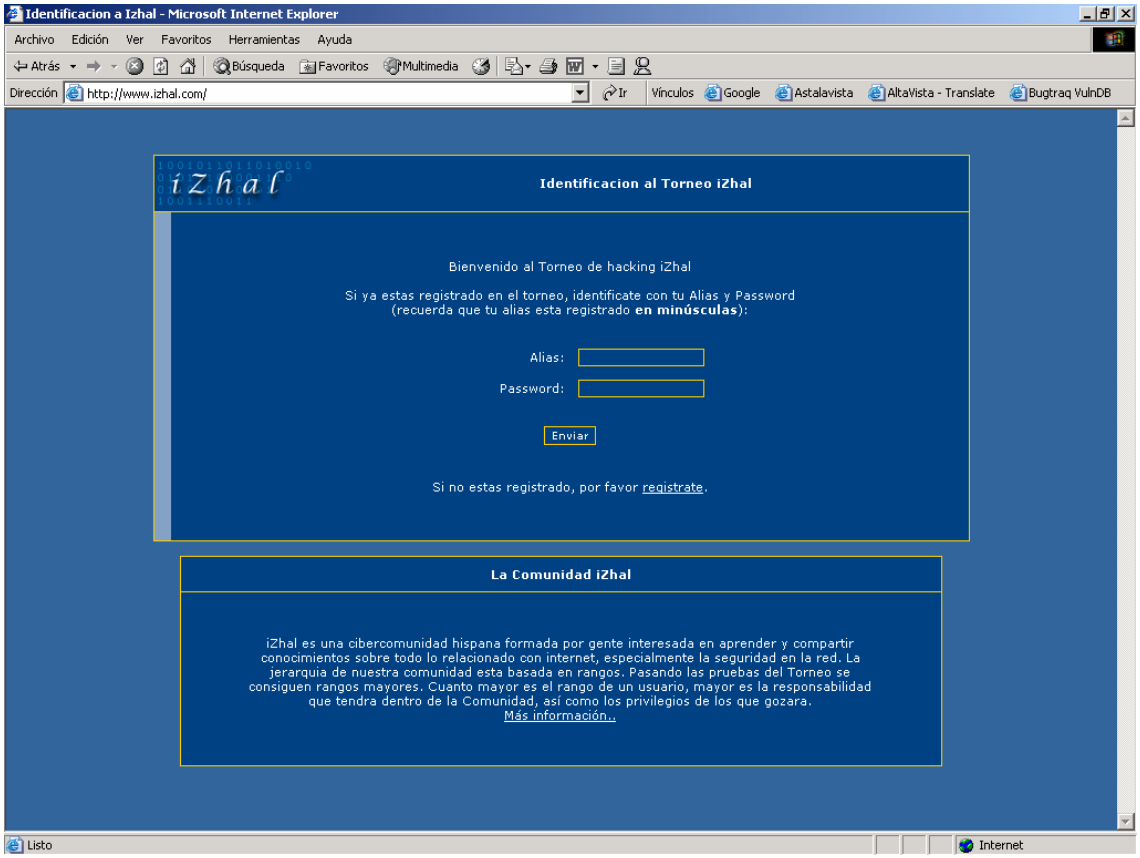


- **Boinas Negras** (http://www.boinasnegras.com): fue realmente un concurso aunque debido a su éxito los organizadores decidieron dejarlo online por un tiempo (y todavía sigue ahí). Principalmente basado en el mundo Microsoft (IIS / SQL Server) y con pruebas bastante reales. Orientado a la autentificación web. En castellano. Muy bueno.

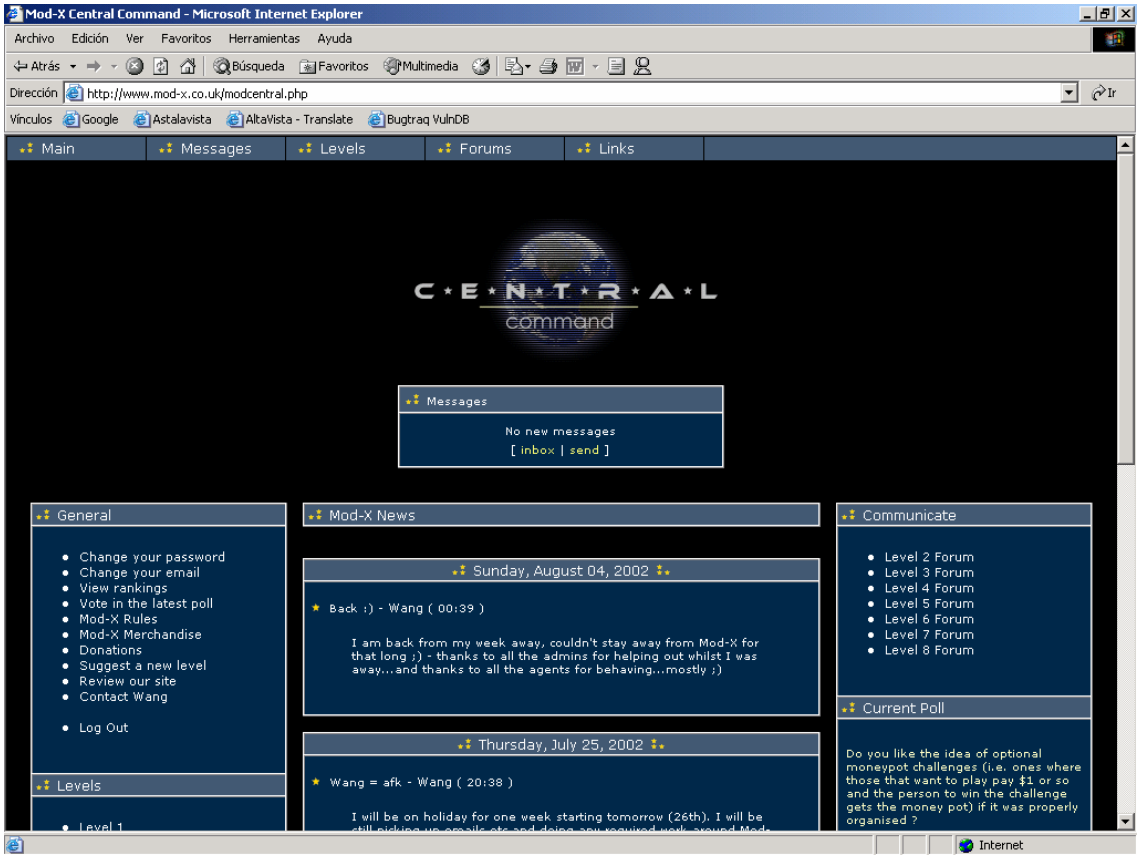
- **Arcanum** (http://www.arcanum.co.nz/): bastante estructurado, cada nivel se compone de cuatro partes independientes que hay que superar para pasar al nivel siguiente: lógica, programación, encriptación y desconocida. Para la parte lógica no es necesario saber de informática ni de hack; son problemas típicos "con truco" o donde simplemente hay que pensar un poco. La de programación consiste en resolver un problema matemático ayudándonos de un programa que debemos escribir nosotros mismos. La de encriptación nos pedirá que descifremos pequeños textos. La marcada como desconocida son pruebas de diversa índole. En inglés. Muy entretenido si te gusta pensar aunque no demasiado técnico.



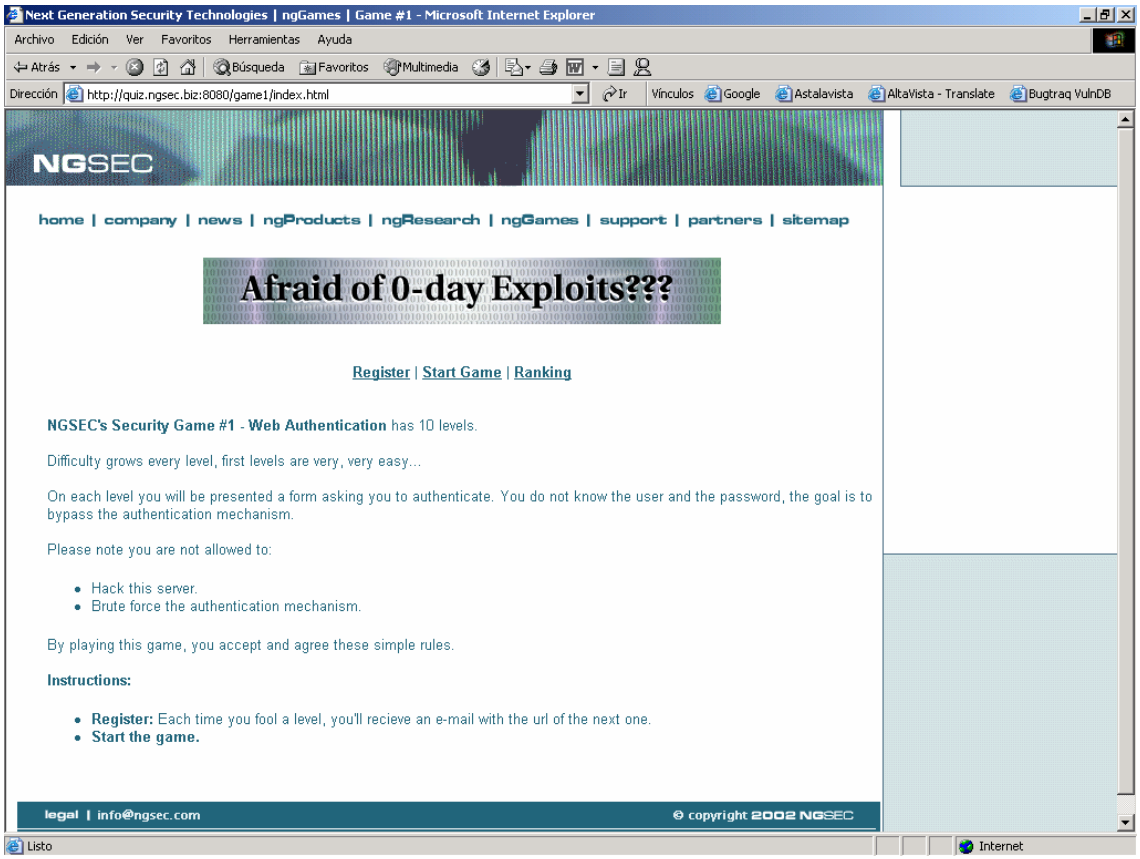
- **iZhal** (http://www.izhal.com/): excelente juego en castellano y al alcance de todos, ya que empieza desde un nivel de principiante y contiene pruebas variadas. Incluye pruebas de entrenamiento. Recomendado para todo amante de los wargames, especialmente para los que pretenden iniciarse en el tema. Probadlo.



- **Mod-X** (http://www.mod-x.co.uk/): pruebas varias un tanto extrañas. Incluso aparece algo de esteganografía. En inglés. Curioso.



- **Ngsec Security Games** (http://quiz.ngsec.biz:8080/): bastante instructivo ya que cada nivel ofrece un enlace a un documento explicativo de la técnica a emplear para la superación del mismo. Orientado a la autenticación web con una cierta tendencia Unix. En inglés.



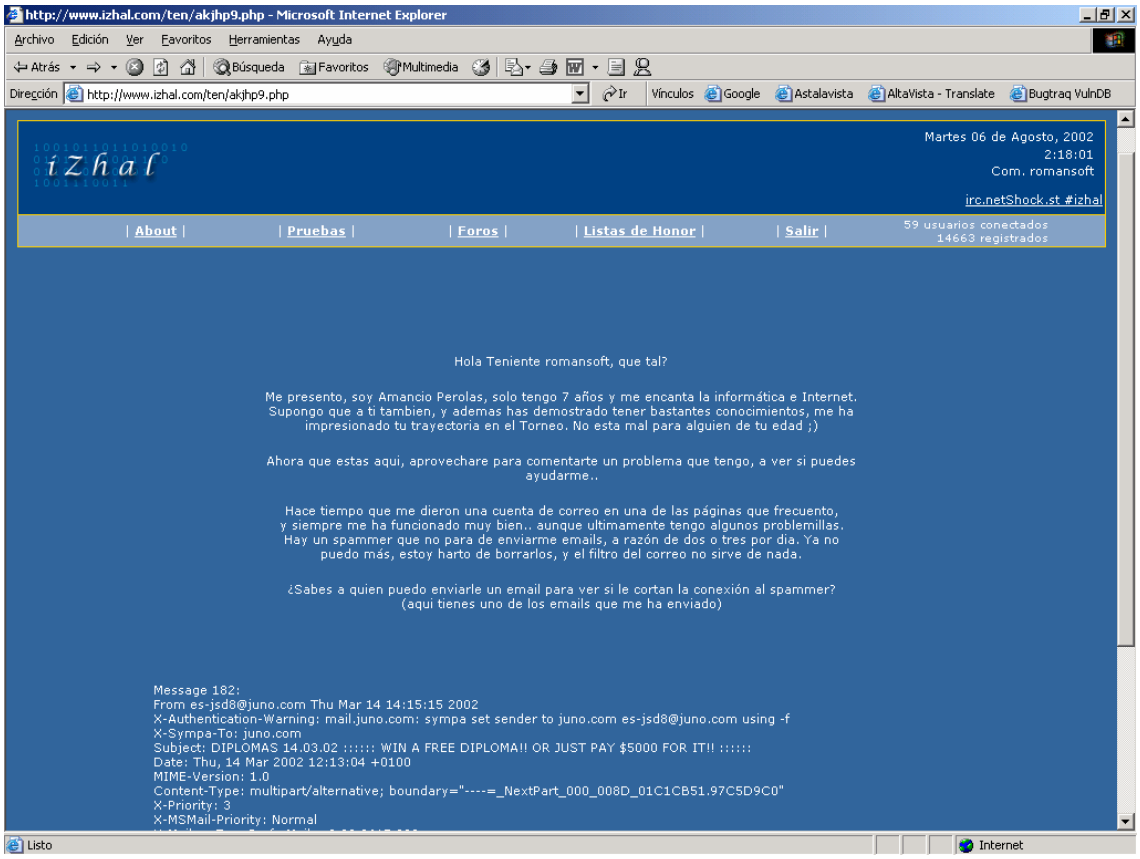
La comunidad iZhal

Para finalizar nuestro recorrido en el tema que nos ocupa y a modo de ejemplo vamos a centrarnos en un wargame en particular. Se trata de iZhal, un juego ideal para alguien que desee iniciarse en este interesante mundillo y que además tiene sello español. Cuenta ya con más de 15000 usuarios registrados, en su mayoría hispanohablantes, lo que constituye una pequeña muestra del gran éxito obtenido.

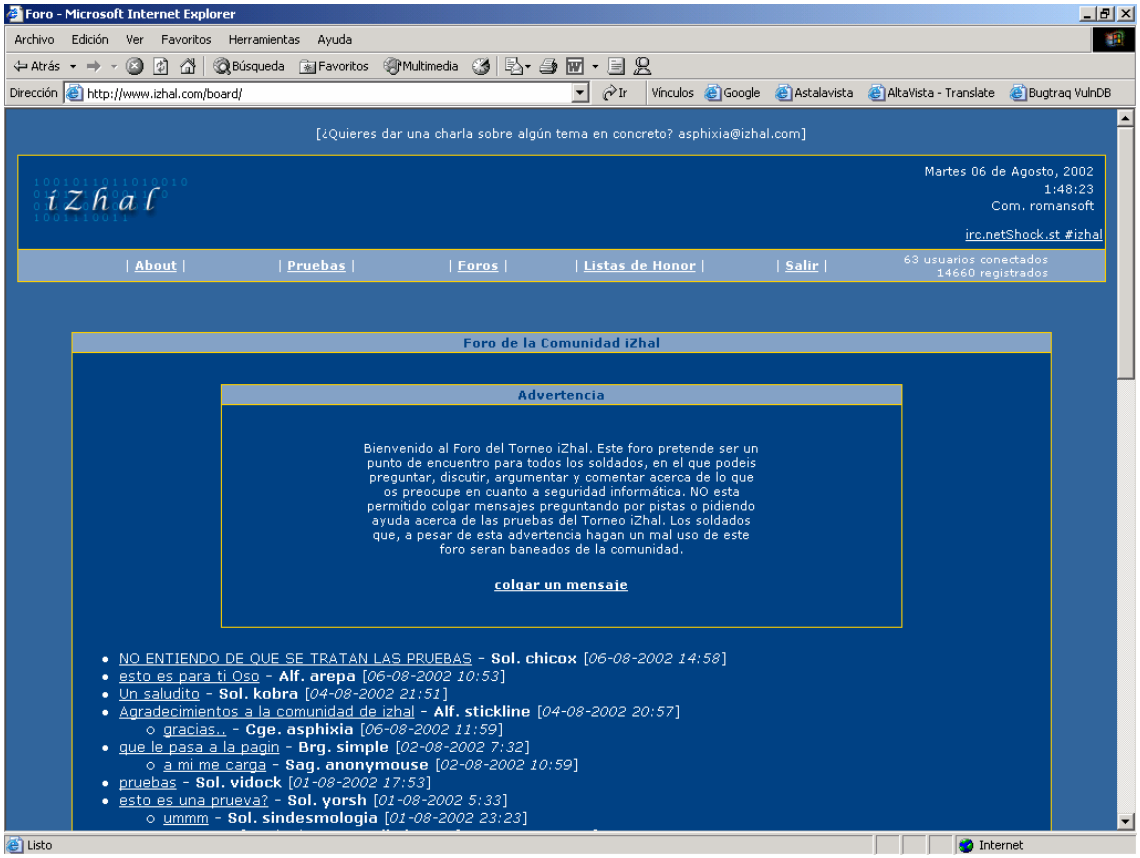
En iZhal se hace corresponder cada fase o nivel del juego con un rango en la jerarquía militar de forma que un participante comienza con el rango de soldado para luego ir ascendiendo a cabo, sargento, brigada, subteniente, etc. Se supone que los rangos superiores tienen mayores conocimientos o al menos han demostrado más pericia (o simplemente han invertido más tiempo) que los participantes con rango inferior. Esto no quiere decir que se trate de un juego elitista y que se menosprecie a los que están por debajo. Nada más lejos de la realidad. Al contrario, los participantes con rangos superiores suelen ayudar en la medida de lo posible a otros participantes que se encuentran en un nivel inferior, y en general se vuelcan más con el juego. También es habitual que participantes de igual rango se enfrenten en conjunto ante determinadas

dificultades u obstáculos y aprendan unos de otros. Esta interactividad es lo que hace que iZhal se convierta en toda una comunidad de personas con intereses, inquietudes y aficiones comunes. La jerarquía forma parte del juego y contribuye a crear una atmósfera especial y divertida o simplemente desemboca en una sana rivalidad entre los participantes que hace que los mismos se esfuercen más y el juego cobre un mayor interés.

Las pruebas incluyen desde típicos ataques de fuerza bruta a un archivo de contraseña de Windows hasta alguna prueba de cracking (entendiendo como tal el destripar un fichero ejecutable y "reventar" alguna de sus protecciones) así como alguna que otra prueba que requiere de conocimientos básicos de criptografía (que se pueden adquirir perfectamente en la etapa de documentación que todo participante debería ejecutar cuando se enfrenta por primera vez a un nivel cuya temática es desconocida para el mismo), pasando por otras que requieren un cierto conocimiento de Internet. El mejor recurso o herramienta que todo participante debería usar es Google. El saber documentarse y encontrar información en Internet es una gran ventaja para afrontar las pruebas o mejor dicho, casi un requisito indispensable.



Disponemos de un foro para cada nivel o rango de forma que participantes de un mismo nivel puedan ponerse en contacto y hablar sobre las pruebas anteriores e incluso discutir acerca de las correspondientes soluciones sin que afecten a los participantes que todavía se encuentran cursando dichas pruebas. Aparte existe un foro de uso general, accesible para todos. Por último, iZhal también dispone de un canal de irc oficial (#izhal en irc.netshock.st) donde los participantes pueden charlar en tiempo real con otros compañeros e incluso con los creadores del juego.



No hay premios pero por ejemplo un teniente puede moderar el foro de soldados y eliminar artículos que consideren improcedentes o no acordes con las normas del juego, o un comandante podrá recibir una cuenta de correo pop3 sin restricciones en el servidor de izhal de forma totalmente gratuita. Es decir, conforme se sube de rango se va ganando ciertos privilegios, lo que constituye un aliciente más.

Con el fin de que nuestros lectores conozcan más a fondo cómo se organiza a nivel interno un wargame y la apreciable labor que requiere llevarlo adelante hemos entrevistado a los dos máximos responsables de iZhal. Creemos que es la manera adecuada de terminar este artículo y esperamos que haya sido de su agrado. ¡Hasta el próximo número! ;-)

Entrevista a “asphixia” y “enraged” -creadores de iZhal-

Rom.- Lo primero de todo me gustaría que os presentaseis. ¿Quienes son asphixia y enraged en la vida real? ¿Aficiones, edad? ¿Nivel de conocimientos informáticos? ¿Cuanto tiempo lleváis en el mundillo “under”?

asphixia.- Pues tengo 21 años, recién licenciado en administración y dirección de empresas, y mi afición por los ordenadores empezó hace muchos años, y se intensificó cuando descubrí Internet cuando tenía 14 años. Inmediatamente empecé a estudiar en diversas academias diseño de páginas web y Visual Basic. Al cabo de poco hice mi primera página web. A partir de ahí ya me empezó a interesar el mundillo “under” en el que es necesario el auto-aprendizaje, al que ya me he acostumbrado y me ha servido también para aprender PHP/MySQL, entre otras muchas cosas.

enraged.- Yo estoy estudiando informática de sistemas en Barcelona, este año empezare segundo curso. En cuanto al nivel de conocimientos informáticos yo no lo consideraría alto ni mucho menos, aunque intento aprender sobre nuevos temas cuando estoy en la red. Al igual que asphixia ya hace bastante tiempo que estoy por internet.

Rom.- ¿Cómo surgió la idea de crear iZhal?
A&E.- Hace tiempo descubrimos cyberarmy.com, un "hacking challenge" americano, y estuvimos realizando las pruebas que planteaban. Empezaron a surgir torneos alternativos en inglés, y decidimos crear uno similar para el mundo hispano en general.

Rom.- ¿Con qué presupuesto contáis? ¿Quién os financia?
A&E.- Aunque hace tiempo estuvimos en contacto con un posible patrocinador, actualmente no nos patrocina nadie. Aun así, debemos agradecer los servicios que nos prestan "elserver.com" y "netshock.st", como servidores de iZhal y de la red de IRC respectivamente.

Rom.- ¿Qué beneficio os reporta iZhal? ¿Por qué lo hacéis?
A&E.- No nos reporta ningún beneficio económico, pero nos ayuda a seguir aprendiendo a medida que vamos programando las pruebas con la colaboración de algunos usuarios, y vamos creando la página en sí.

Rom.- ¿Hay proyectos parecidos a iZhal en España? ¿Qué tiene de innovador iZhal?
A&E.- Después de iZhal han surgido algunas páginas parecidas, pero ninguna de ellas ha captado tanta gente, pese a ofrecer premios. La cuestión reside en que iZhal es una comunidad en la que los organizadores estamos al mismo nivel que los participantes, es decir hablamos entre nosotros, detectamos y arreglamos errores en la página, diseñamos nuevas pruebas para el torneo… Digamos que en iZhal el usuario es parte de la página y puede aportar su grano de arena, mientras otras están conducidas por empresas y son mucho más rígidas.

Rom.- ¿iZhal no es un concurso? ¿Por qué no hay premios?
A&E.- Estamos pensando en diferentes maneras de ofrecer premios a nuestros concursantes. De momento intentamos dar como premio privilegios en la página, como la posibilidad de moderar foros, e-mail pop3, status en el IRC, etc.

Rom.- ¿Cual creéis que es la clave del éxito que está teniendo iZhal?
A&E.- Más que éxito es la organización de la página en sí que atrae y mantiene a los visitantes ya que no es un torneo con 12 pruebas cerradas y punto sino que cuando estén acabadas todas las pruebas habrá pruebas temporales con premios para los más rápidos. Además es una página en la que es fácil integrarse y colaborar. Digamos que cada uno puede extraerle todo el jugo que quiera.

Rom.- ¿Qué nivel de conocimientos son necesarios para superar las distintas pruebas de iZhal?
A&E.- El torneo empieza con un nivel muy elemental (de hecho hay un entrenamiento) y va subiendo gradualmente. En pruebas de niveles más altos ya son necesarios conocimientos de ingeniería inversa, criptografía y algún que otro lenguaje de programación.

Rom.- ¿Tenéis en mente mejoras o nuevos proyectos?
A&E.- Tenemos en mente muchas mejoras y proyectos para iZhal, como por ejemplo la construcción de un portal con descargas, tutoriales, enlaces y noticias. El objetivo es ofrecer más contenidos en la página, para que no se limite solo al torneo de hacking. Asimismo también hay otros proyectos planeados, como la construcción de pruebas temporales con premios, la creación de grupos de trabajo y estudio sobre diferentes temas (brigadas), etc.

Rom.- ¿Contáis con algún tipo de ayuda externa o cargáis vosotros solos con todo el peso de iZhal?
A&E.- Son muchos los que nos ayudan con el mantenimiento y la construcción de la página, sobre todo los que consiguen llegar a los niveles superiores del torneo, que normalmente son los que más se involucran. De todas formas iZhal podría crecer mucho más si contásemos con el apoyo de organizaciones que pudiesen patrocinar algunas pruebas para ofrecer premios a los participantes.

Rom.- ¿Qué consejo le daríais a los participantes del torneo iZhal?
A&E.- El torneo está planteado para ir aprendiendo a medida que se van superando las pruebas. Cuando un usuario llega a una prueba que en un primer momento no sabe superar, no debe desanimarse ni pedir la solución; ahí es donde los participantes deben usar el auto-aprendizaje. Con la incorporación del portal ya habrá un fondo de tutoriales en la propia página pero mientras tanto no es muy difícil encontrar información y lectura sobre los temas que tratamos en las pruebas. Además en los foros se puede intuir muchas cosas: aunque no se permita discutir las pruebas en sí hay información que puede ser útil para enfocar las pruebas.

Rom.- Si queréis añadir algo más para cerrar la entrevista...
A&E.- De alguna forma nos gustaría agradecer la ayuda que prestan desinteresadamente a iZhal todos los que han ayudado en la construcción de la página, ya sea con ideas y sugerencias, hasta los que se han atrevido a plantear y crear alguna prueba del torneo. También aprovechamos la ocasión para hacer un llamamiento a posibles patrocinadores para potenciar la página con alicientes para los participantes.

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

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