UN INFORMÁTICO EN EL LADO DEL MAL

Spectra, Técnicoless, Técnico-Less, Blind SQL Injection, LDAP Injection & Blind LDAP Injection, Retos Hacking, Metadatos, FOCA, Cursos de Seguridad Informática, Eve Conferencias, MetaShield Protector, Connection String Attacks, Maligno, Spectra, Seguridad Informática, Hacking, tocar los webos...y Chema Alonso.

LUNES, MARZO 23, 2009

Entrevista a RoMaNSoFt

Durante mucho tiempo RoMaNSoFt era una marca que te encontrabas en sitios dónde menos te los esperabas. Unas letras en 3D antes de algún juego. ¿Quién es este tipo? Después, un día, pasa por tu blog y te deja un comentario. ¡Coño! ¿será el mismo? A este tipo le tengo que conocer. Así fue como después de algún reto hacking logré quedar con él en los madriles para tomar un café y charlar... y me encuentro a Román.

Román es adorable. Sí, es como un niño travieso hiperactivo, con timidez subida y mirada nerviosa. Gesticula al tiempo que habla, se ríe y se sonroja. Cuando se habla de algo que ha hecho él se le suben los colores y sonríe nerviosamente como si el estar en el centro del escenario le pudiera. Es hasta divertido sacarle los colores. El acento del sur que le acompaña hace de todo él un tipo genial y divertido.

RoMaNSoFt asombrado con su movil...

La segunda vez que nos juntamos, que fue la primera vez que conocí a Palako, tuvo lugar en una cervecería. Se vinieron a aquella reunión también Ricardo Varela, Atar, Rodol y Antonio Guzmán (todo un elenco). Y recuerdo como durante una conversación que tenían sobre la clave de una Wifi Román se quedó *"enganchado"* mirando al techo. *"¿Qué haces Román?" "Na',na', calculando el tiempo en romper una clave así".*

En otra cena, el día antes del Asegúr@IT I, para el que había conseguido liarle y que cantara, quedamos en casa Mingo, en Madrid. *"Aparca en el centro comercial de Príncipe Pio y vente andando Roman, es poco." "¿A qué distancia está?" "Pues... a unos diez minutos a pie" "no, no, distancia en metros" "Pues... unos 600 metros"."mmm, vale, a unos 7 minutos andando".* Así es Roman, un cerebro privilegiado, metido en el alma de un niño travieso y tímido.

Entañable.

1.- ¿Cuál fue tu primer encuentro con la informática?

No es fácil de recordar... era pequeñito... tendría unos 10 años :) Pero fue con un invento del mítico Sir Clive Marles Sinclair. Como no, se trataba del famoso Spectrum 48K ("el de las teclas de goma"), que modestamente no servía para mucho más que jugar pero que desde el primer momento despertó mi curiosidad. Aprendí BASIC con él, en parte debido a los gazapos que introducían las revistas de la época

De profesión: Sus labores
Asegúr@IT V - Online
Serialized SQL Injection (Parte III de VI)
Vídeos y audios de la Defcon16
Exportando "sexy" Pandas
2008, una gran cosecha
Vida de feriante por los pueblos del Sur
Ánimo Pandas!
El mundo es de papel
El full-ekip
Serialized SQL Injection (Parte II de VI)
Tipos de informáticos: Momento Sexpeme
Serialized SQL Injection (Parte I de VI)

► febrero 2009 (31)
► enero 2009 (32)

► 2008 (521)
► 2007 (412)
► 2006 (147)

SEGURIDAD APPLE

Cargando...

WINDOWS TÉCNICO

Cargando...

SEGUROS CON FOREFRONT

Cargando...

BLOGS Y LINKS

- Informática 64
- Infospyware
- Windows Técnico
- Seguros con Forefront
- Seguridad Apple
- El Blog de Thor
- Campaña Hands On Lab
- El Blog de Cervi
- Blog Héctor Montenegro
- Juan Luís Rambla
- Punto Compartido
- Exchange Spain
- Silverhack
- Security By default
- elhacker.net
- Conexión Inversa
- Seguridad y Privaciad
- Bank of Maligno - Login
- Cyberhades

RETOS HACKING

Primera Temporada
- Reto Hacking I

BASIC con él, en parte debido a los gazapos que introducían las revistas de la época (realmente no recuerdo si había vida más allá de Microhobby) en los listados de los programas que incluían. Rara vez funcionaban a la primera lo que me obligaba a realizar pequeñas correcciones.

Al mismo tiempo mi padre se compró un Amstrad CPC6128, para trabajar. La idea era que mis hermanos y yo nos entretuviéramos con el "Speccy" y nos mantuviéramos alejados del CPC. No lo consiguió y al poco tiempo yo ya dominaba el BASIC del CPC (que era muchísimo más potente que el del Spectrum), algunos que otros truquitos como llamadas a subrutinas especiales (call &bb18 ...) y posteriormente un poco de ensamblador. Realicé por completo un programa de gestión de laboratorio, que es posible que todavía esté en producción ya que lo fui migrando a diferentes plataformas, pasando por el Amstrad PCW hasta el PC que todos conocemos.

También desprotegía juegos y hacía algo de trading (a pequeña escala; apenas me servía para financiar la compra de discos vírgenes). Fue a lo largo de esa época cuando se forjó el sello de "Roman Soft" (por razones obvias). Se fue haciendo poco a poco conocido por lo que me daba pereza cambiarlo. Al final todavía hoy lo mantengo (escrito como "RoMaNSoFt").

Luego tuve una segunda época muy fructífera con el Commodore Amiga. Me empollé el "Amiga Hardware Reference Manual" (de los primeros libros en inglés que recuerdo haber leído) y me lancé a la programación en 68000. Llegué a formar parte de uno de los grupos más prestigiosos de la scene nacional (LLFB -algunos los recordarán por su docs-), como programador ("coder" sonaba más cool) e hice un par de intros y alguna cosa que nunca llegué a publicar/terminar. Realmente era duro programar una intro en ensamblador ("ASMOne" rlz :)) partiendo de cero, sin ninguna librería gráfica o matemática y con el objetivo de aprovechar al máximo los escasos 7 MHz de CPU que tenía el Amiga. Pero esa era la gracia: tablas de seno/coseno a capón en el código, implementación de la matriz de rotación necesaria para efectos 3D, "double buffering", "clipping", optimización de código "manual" (nada de compiladores)... y muchas otras curiosidades. Se conseguían efectos muy suaves cuando en el PC de entonces ver un scroll que no fuera dando saltos era toda una proeza.

Pero de PC también había que saber así que, en paralelo, me puse al día con el MS-Dos (el Win 3.11 lo arranqué alguna vez pero realmente no lo llegué a utilizar en serio; comparado con el Workbench del Amiga, Win daba pena), scripting .bat y algún que otro cachondeo añadiendo alt-255 a ficheros y directorios para "impedir" el acceso a los mismos. El profe de informática creía que los diskettes tenían virus (bueno, a eso hay que añadir que intercambiamos -físicamente- las teclas Ctrl y Alt del viejo teclado de los IBM PS/2).

Estamos hablando del año 93 ya...

2.- ¿Y con el mundo de la seguridad informática?

... por aquel entonces entré en la Universidad. Coincidió más o menos con una serie de artículos de HPCV que leí en la revista digital de la escena española del Amiga ("Fanzine"), donde hablaban de terminales, monitorización de procesos y hasta de blue-boxing (el controvertido artículo de "Agnus Young"). Conseguí mis primeras cuentas tanto en Ultrix como en VMS. Me enamoré de Unix y comencé a aprenderlo a base de "man ". Un día en la residencia vi a un compañero de un curso superior con un libro muy gordo que me llamó la atención y se lo pedí prestado. Su título: "Unix System V Release 4" (Rosen). Me lo leí de cabo a rabo.

Sistemas multiusuario, contraseñas encriptadas, permisos de ficheros, un potente sistema de scripting... simplemente genial para alguien que venía del mundo monousuario y con sed de aprender cosas nuevas. Ni qué decir tiene que la seguridad en aquella época brillaba por su ausencia: filesystems montados por NFS, /etc/passwd con contraseñas (shadow, ¿qué era shadow?), NIS... el paraíso del hacker ;-)

El acceso a Internet estaba muy limitado... tanto que nuestras cuentas de alumnos no tenían ni acceso web (/gopher) ni siquiera e-mail (qué triste) así que me construí un sencillo sistema de mensajería basado en shell (bourne shell) para intercambiar mensajes con mis compañeros. Utilizaba un directorio en cada home, con permisos especiales, que hacía las veces de spool. El sistema era "relativamente" seguro (todo lo seguro que puede ser un sistema así, se entiende) y lo mejor de todo, funcionaba. Pero no gustó a los administradores, que me acabaron llamando la atención. No quiero generalizar pero muchos de los sysadmins de aquella época eran meros funcionarios que hacían lo justo para que sus sistemas se mantuvieran en pié; no controlaban de seguridad ni parecía interesarles demasiado. Simplemente miraban algún que otro log y si descubrían, por ejemplo, una cuenta de usuario compartida, la cerraban. Los usuarios eran muy inocentes; frecuentemente te encontrabas con sesiones abiertas en el terminal vt100 (los PCs eran muy caros todavía para ser usados como terminal...), por

- Marathon Tool
- Thumbando
- WbFingerprinting
- i64SSLPOP3Connector
- LDAP Injector
- LISSA 2k
- LISSA 2k4
- CSPP Scanner

ETIQUETAS

Seguridad Informática (750)
Eventos (467)
Curiosidades (394)
Hacking (386)
Spectra (197)
Humor (183)
Google (153)
Internet (152)
Linux (126)
Reto Hacking (125)
Comics (115)
No Lusers (107)
Metadatos (104)
Windows Vista (95)
Blind SQL Injection (73)
SQL Injection (73)
FOCA (68)
Windows Server (60)
Fingerprinting (58)
PCWorld (52)
Apple (51)
Software Libre (51)
Firefox (49)
Técnicoless (49)
Técnico-less (46)
Windows 7 (44)
Wireless (44)
Oracle (43)
Estafas (42)
IE (42)
Ubuntu (42)
Malware (41)
email (41)
Entrevistas (39)
OOXML (37)
Open Source (36)
Spam (36)
Windows XP (36)
Office (35)
Herramientas (34)
XSS (34)
Blind LDAP Injection (33)
ODF (33)
SQL Server (33)
Análisis Forense (29)
Apache (29)
Calendario_Torrido (29)
LDAP (29)
LDAP Injection (29)
BING (28)
IIS (25)

desconocimiento.

Al año más o menos tuve acceso al correo electrónico y a las news. Corrían los tiempos del "elm" y del "pine" (y de los agujeros de sendmail...). Me suscribí a diversos grupos de Netnews, incluído es.comp.hackers (nada del otro mundo pero era lo que había). Comenzaron los primeros piques...

Absorbía documentación... Me bajaba archivos gracias a pasarelas "ftpmail". No teníamos acceso a ftp, ni siquiera a www. Más tarde, abrirían un penoso canuto por el que dejaban bajarse contenido web a "increibles" tasas como los 200 bytes/segundo (no, no me he olvidado ninguna "k"). Nos sabíamos todos los atajos del "lynx", qué desesperación :)

*El teléfono era caro y yo vivía en una pequeña (y gran) ciudad por lo que no tenía acceso a ninguna BBS. Menos mal que llegó el boom de los ISP e Infovía. Los 28.8 kbps de mi modem junto al Netscape Communicator me sabían a gloria. Eran los tiempos de webs como "rootshell" y del IRC. Conocí a mucha gente, estaba enganchado a este último y tenía un PC con RedHat 4.2, lleno de artillería pesada. De esta etapa nacería mi conocido artículo de "Tácticas de guerra en el IRC". Los usuarios, con sus Win95 con recursos compartidos, desfilaban por la red de redes ofreciendo generosamente su perfil de "acceso telefónico a redes", lo que permitía obtener el usuario y contraseña del ISP. Aunque muchas veces no eran necesarios: los ISPs utilizaban CGIs peligrosos, que posibilitaban la obtención de las contraseñas (encriptadas) de *todo* el ISP... La conocida tool de Alec Muffet echaba humo. ¿Quién no recuerda a "Crack"?*

Incluso en esa etapa más o menos oscura que todos hemos tenido jamás borré un home ni obtuve beneficio económico alguno. Simplemente me limité a aprender todo lo que pude, sin hacer daño a nadie.

3.- Siempre has sido un poco polémico, que si le das caña a Hispasec, que si le das caña a S21Sec, que si paso "no-se-qué" en boinas negras, que si el Reto Hacking de el lado del mal…¿cómo es que no te han partido las piernas aun?

Esta pregunta va con trampa, ¿verdad? Vamos por partes. Creo que no es malo ser un poquitín polémico (siempre en su justa medida, claro). Significa que estás vivo, que no eres un mero espectador: cuestionas las cosas, las analizas con conocimiento de causa y por último las criticas constructivamente. La diferencia estriba en el sentido que uno le de a esas críticas y si éstas son o no fundadas. Respecto a lo primero, mis críticas nunca han pretendido herir a nadie (y si alguien se ha sentido ofendido, que me perdone O:-)) sino que pretenden llamar la atención para que se mejoren las cosas. Sobre lo segundo, decir que como buen teleco me considero bastante calculador y estricto. Me puedo equivocar, como no, pero soy de los que "pierden el tiempo" en repasar las cosas una y otra vez, antes de darlas por válidas, buscando una calidad más que aceptable y reconozco que me fastidia cuando otros no lo hacen así (que por otro lado y por desgracia, es lo normal) y por su culpa acabo perdiendo mi valioso tiempo. Te pongo un ejemplo: ¿qué pasa cuando pierdes un dia intentando romper un nivel de un reto y luego resulta que ese nivel no se podía superar porque estaba mal programado? ¿Y si eso mismo ocurre de forma reiterada? Incluso haciendo uso de mis más malignas tácticas (como dejar a Kachakil ir por delante, abriendo paso y reportando esos fallos), al final te acabas cabreando...

Por otro lado, mi "lista de polémicas" no es tan grande :-))) Casi que las has resumido en el enunciado de la pregunta, no sé si merece la pena entrar al trapo (son "públicas", si sabes buscar en Google y en listas de correo). Tanto Hispasec como S21Sec son empresas de conocida solvencia en el panorama nacional de la seguridad y tengo buenos amigos que están en (o han pasado por) ellas. Pero también pueden llegar a ser criticables ya que nadie es perfecto. Y hasta aquí puedo leer :-#

4.- ¿Cómo has aprendido seguridad informática? (y no me digas leyendo aquí y allá)

Pues no te lo digo (porque ya lo has dicho tú...). Siempre he sido autodidacta. El secreto está en cuestionarte todo... ¿cómo o por qué funciona tal cosa? ¿Qué ocurre si modifico...? ¿Cómo se podría mejorar...? Lo podría resumir en tres palabras: "leer", "cacharrear" y "tiempo".

5.- ¿Cómo te dejaste liar para cantar en el Asegúr@IT I con lo tímido que eres?

Uf, ya te vale. Un gran secuaz de Spectra nos engañó a todos... Este maligno ser le dijo a Kachakil que yo iba a "cantar" (como tú lo llamas); y a mí me dijo lo propio de Kachakil. Y así fue haciendo con todos los ponentes de forma que cada uno pensaría: "pues si los demás lo hacen, yo también". ¡Te quedaste con todos, mamonazo!

6.- ¿En cuántos retos hacking has participado? ¿Cuál ha sido el que más te ha entretenido?

He participado en muchos, sería imposible acordarme de todos. Algunos ejemplos: cyberarmy, izhal, hackerslab, arcanum, mod-x, los tres boinas negras (en realidad eran dos y medio; el tercero fue interrumpido), los dos hack21, yoire, blindsec, los dos ngsec, prequals de Defcon y de Codegate 2009... y hace unos días me apunté a uno de los antiguos retos de pulltheplug (Vortex). En todos he aprendido algo. Recuerdo como altamente técnico y real el de hackerslab pero el que más me ha entretenido fue el primer boinas negras (por el tipo de reto, singular premio y sobre todo por la época... estuvo muy bien organizado e implementado -Gonzalo se lo curró- y tuvo una muy buena acogida).

¿Para cuándo un Boinas #4? ¿O un Hack21 #3? Se lo tendrás que preguntar a Gonzalo o a Barroso cuando los entrevistes un día de estos...

7.- ¿En cuántas listas de correo estás suscrito?

Bastantes, aunque no las leo todas; sí las "reviso" por encima. Entre las más atractivas destacaría Dailydave, las de Securityfocus y alguna que otra privada (si te lo contara te tendría que matar...). De todas formas, con la proliferación de los blogs y los RSS es fácil mantenerse al día sin leer ni una sola lista de correo; de los blogs españoles me gustan, entre otros, el de S21sec, Hispasec, SbD y cómo no, el tuyo. Lo suyo es combinar todas las fuentes: listas de correo y blogs.

8.- ¿Cómo te apañas para recordar los nicks de todo el mundo y saber lo que han hecho y han publicado?

No exageres, mi memoria no es tan buena. Tendría que ampliarla... Pero sí es cierto que me gusta seguirle la pista a mucha gente, tanto española como extranjera.

9.- ¿Has probado ya Windows 7?

No. ¿Y tú Debian 5? :-) Desde hace muchos años mi política respecto a Windows ha sido la de ir siempre una versión (o en su defecto, algunos Service Packs) por detrás; la experiencia ha demostrado que me puedo ahorrar algunos disgustos. Actualmente estoy contento con XP para el desktop, con Debian para servidores y diferentes live-cds para menesteres varios (pen-test, etc).

10.- ¿Cómo es posible que te hicieran un exploit para un exploit que habías hecho tú?

"Me alegra que me hagas esta pregunta...". Nos remontamos a Marzo de 2003, fecha en la que publiqué mi exploit (rs_iis.c - http://www.rs-labs.com/exploitsntools/rs_iis.c) para IIS 5/Webdav. Llegó a ser tremendamente conocido y referenciado incluso en libros (por ejemplo, en el "Network Security Assessment" de Chris McNab, si no recuerdo mal).

*Introduje un buffer overflow *a drede* y lo *documenté* en el código:*

"// This code is not bullet-proof. An evil WWW server could return a response bigger than MAXBUF
// and an overflow would occur here. Yes, I'm lazy... :-)"

Se trataba de una especie de backdoor documentado. La idea era, por un lado, provocar (ya sabes, me gusta polemizar... y por tu pregunta veo que lo conseguí), y por otro, tener a mano una pequeña salvaguarda, en caso de que los "script-kiddies" se pasaran de la raya lanzando el exploit a diestro y siniestro. Realmente no pensé que nadie se molestaría, más tarde, en construir el "exploit" que aprovechara dicha puerta trasera. Y aún menos que algunos aprovecharían todo esto para criticarme, bien por desconocimiento o incluso con cierta malicia.

11.- ¿No te dijeron nada los de Debian por ser tú el que programó el exploit con que tiraron Gluck?

Primero he de aclarar que yo sólo soy coautor del exploit (rs_prctl_kernel.c - http://www.rs-labs.com/exploitsntools/rs_prctl_kernel.c), y que de hecho la parte principal del mismo es obra de dreyer (ver cabecera/comentarios del exploit). En todo caso, ¿por qué nos tenía que decir nadie nada? Nosotros no tuvimos nada que ver con ese hackeo (ni con ningún otro).

12.- ¿Cuál ha sido el mejor libro de seguridad que has leído?

Tengo una amplia colección, me gusta además tenerlos en papel, en parte por comodidad, en parte por colaborar con los autores (salvo excepciones -algún bestseller- escribir un libro técnico no creo que compense económicamente y si que

conlleva mucho trabajo).

Para que te hagas una idea del tipo de libros que me gustan (no creo que te sorprenda...) echa un vistazo a mi wish-list de Amazon: http://www.amazon.com/gp/registry/wishlist/SYOS7ANC7UNO/ref=wl_web&sort=priority/
La puse en mi web (http://www.rs-labs.com/) hace tiempo, por si a alguien le gusta lo que publico o lo que hago y me lo quiere agradecer pero se ve que no... :) Así que la utilizo para tener fácilmente localizables algunos libros interesantes y que todavía faltan en mi biblioteca.

Un libro que me gustó mucho es: "Hacking, the art of exploitation" (Jon Erickson). Yo tengo la primera edición pero creo que ya va por la segunda. Una muy buena referencia como iniciación al "exploiting" aunque advierto que hay que tener cierta base (programación, arquitectura, sistemas operativos...)

Otro que tiene muy buena pinta (al menos lo que llevo leído) es "The IDA Pro book" (Chris Eagle, eterno rival de los "Pandas" :P). Denso, organizado y muy bien explicado. Me encantaron las páginas que describían las "stack frames" en detalle ("calling conventions" y "local variable layout") para diferentes compiladores u opciones de compilación.

De todas formas, los libros están bien pero a veces son más amenos los papers y presentaciones de conferencias como BlackHat, Defcon, CCC...

13.- Si no hubieras sido informático.. ¿de qué hubieras acabado currando?

No sé, fontanero, electricista... quién sabe, son un chollo: hay que rogarles para que vengan, te cambian una pieza y te cobran una pasta (y la mitad no lo declaran). También es un chollo ser "maestro", por la pila de vacaciones que tienen. Ahora en serio, cualquier trabajo "no informático" sale más rentable y estará mejor valorado. ¿Por qué ningún amigo que sea albañil te va a hacer un tabique gratis pero tú sí tienes que ser el g* que limpie los virus, configure el acceso a Internet o mire por qué no arranca su ordenador?

14.- ¿Cuántos equipos tienes en casa?

Pues ahora mismo... 4 portátiles diversos, 2 PCs, 1 AlphaStation 400, 2 Netra T1, 1 SPARCstation 20 y un HP Visualize C3600. También un par de routers Cisco (2503 y otro de la serie 800). En cuanto a SOs: Linux, WinXP, Tru64, Solaris y HPUX. Me falta AIX (tuve un tiempo una RS6000 prestada pero no la pude echar a andar: creo que estaba estropeada) e Irix (las SGI se veían en mis tiempos de Uni, ya están descatalogadas).

15.- ¿Cuál es tu rutina para estar informado al día?

Todos los días reviso lo último publicado en listas de correo y blogs. Para estas últimas utilizo "Google Reader" (RSS) y para las listas tengo creados muchos filtros en mi servidor de correo (Sieve es una maravilla). De esta forma tengo todo ordenadito, esté donde esté, sin depender de filtros en el cliente de correo (que sólo valen para *un* cliente de correo). Soy humilde y no tengo 3G así que nada de iphones, blackberries y demás... (en España las telecomunicaciones son un robo a mano armada, estamos a la cola de Europa).

Es importante quedarte con la copla de las vulnerabilidades y exploits que van saliendo. A lo mejor en el momento no te es útil pero quién sabe si en el siguiente test de intrusión te encontrarás tal o cual servicio corriendo y entonces dirás: "ajá, ¿esto no era vulnerable?"...

16.- ¿Qué le recomendarías a alguien que quiera aprender seguridad informática?

A menudo me encuentro en mi buzón un mail de alguien anónimo que me pide ayuda y me formula esa pregunta. Mucha gente piensa que le recomendaré un par de textos, se los leerán y "ya serán hackers". Eso es imposible. Siempre contesto todos esos correos pero como comprenderás con respuestas más o menos genéricas. Algunos consejos:

- "Seguridad informática" es un término muy general. ¿Sobre qué sistemas/arquitecturas/tecnologías? Si no lo tienes claro puedes empezar leyéndote algún libro tipo "Hacking exposed" que te habla un poco de todo.

- Cuando tengas claro qué te gusta más y por dónde quieres empezar busca información (papers, libros) sobre *esa* temática y *céntrate* en ella. Es un error intentar abarcarlo todo, sobre todo cuando se empieza.

- Busca gente que esté en tu misma situación y tenga los mismos intereses e inquietudes, para compartir dudas/ideas. Aprender en grupo es más divertido

inquietudes, para compartir dudas, ideas. Aprender en grupo es más divertido.

*- Debes dominar *al menos* un lenguaje de programación. Más tarde o más temprano necesitarás automatizar tareas o comprender aquel fallo de seguridad que estás intentando explotar (en mi caso he programado en C, Bash, Perl, Asm, PHP, Python...)*

- imprescindible conocer TCP/IP así como los protocolos más importantes (HTTP, FTP, SMTP, ...).

- Estudia la tecnología que deseas explotar. Antes de "aprender seguridad", hay que "aprender sistemas y redes" :)

- Móntate un pequeño laboratorio con Vmware. Instala diferentes sistemas operativos con versiones no parcheadas y atácalos. También son útiles los live-CDs. Para aprender, está bien "DVL" (http://www.damnvulnerablelinux.org/). Como recopilatorio de tools, la "BackTrack" se lleva la palma. Para temas WiFi prefiero "WifiSlax" / "Wifiway".

- Por último, participa en retos ("wargames").

17.- ¿Quién te ha impresionado en este mundillo?

Muchísima gente. De la escena internacional algunos de mis favoritos son "HD Moore", Michal Zalewski y Alexander Sotirov. En España también hay muy buenos researchers pero sería injusto dar nombres (porque seguro que me dejaría muchos en el tintero). Bueno, voy a dar sólo uno: "dsr" ;-)

18.- ¿Qué es peor aguantar al que te gana en un reto hacking o al Dab cuando se pone a dar guerra?

¡¡A Dab, sin duda!! :-) Además, la gente de los retos no sólo no dan guerra sino que somos como una piña: nos conocemos y ayudamos todos. ¡¡¡El único que intenta picarnos eres tú!!! (por cierto, a ver cuándo tienes el "valor" de participar en uno, vas a ver lo que vale un peine :-P).

19.- ¿Cuándo vas a dejar de ser un "panda adoptado" para dar el siguiente paso?

Tuve mi oportunidad antes de que se formara el grupo, esto es, allá por el 2007 pero el objetivo era ir a competir a Las Vegas (Defcon #15) y aunque por un lado la idea era/es muy atractiva, pegarte un viaje así y acudir a uno de los mejores congresos de seguridad del mundo, y acabar "perdiéndotelo" por participar en el CTF me parecía un tanto desproporcionado. Las "prequals" son también muy divertidas e interesantes y no te tienes que mover de casa :)

En todo caso tengo la suerte de conocer a casi todos los "pandas" y agradezco que me permitan estar a su lado de vez en cuando aportando mi granito de arena.

20.- ¿Dejará RoMaNSoFT Madrid para volver al sur?

Ya me gustaría a mí... pero no es fácil: tendría que encontrar un curro interesante, estable y bien pagado. Y eso en Andalucía, es harto difícil, hay demasiado "garrulismo". No me resigno pero hay que ser realista (quién sabe, lo mismo algún día...)

PUBLICADO POR MALIGNO A LAS 9:30 AM

ETIQUETAS: ENTREVISTAS

16 COMENTARIOS:

tayoken dijo...

Eres un fiera ;)

23/3/09 11:21 AM

Alejandro Ramos dijo...

Joder Roman, casi me casca el FF cargando tus parrafadas...

¿y como que dab? yo soy buena gente :(

Por cierto, muy divertida!

23/3/09 12:46 PM

switching (1)
wikileaks (1)
winsocket (1)

Daniel dijo...

Pregunta numero 13.... solo decir, por de más cierto..

23/3/09 1:18 PM

Dani Kachakil dijo...

¡Qué gran entrevista! La verdad es que yo me la esperaba en dos partes, jeje. Sí, Román se enrolla bastante, pero es que siempre da gusto leer o escuchar lo que cuenta (ya sea por mail o en persona... es todo un placer).

"...como dejar a Kachakil ir por delante, abriendo paso y reportando esos fallos"

:-D Te ha faltado tu frase típica de "Kachakil coge el Visual Studio y en 5 minutos nos gana a todos el muy c******". Y eso que en la mayor parte de los casos lo suelo hacer a mano y acabo antes. ;-)

También corroboro esta frase, con la que también me siento identificado, obviamente:

"Este maligno ser le dijo a Kachakil que yo iba a "cantar" (como tú lo llamas); y a mí me dijo lo propio de Kachakil"

Jeje, es cierto que Chema es un liante (en el buen sentido de la palabra), pero hay que reconocer que es muy bueno en ello y que gracias a eso hemos podido disfrutar (y seguiremos haciéndolo) de un sinfín de eventos, charlas, entrevistas, etc. Aquél AseguraIT fue toda una experiencia y yo creo que lo volvería a hacer sin pensármelo dos veces.

¡Saludos!

23/3/09 2:00 PM

enraged dijo...

Vaya tela el RoMaNSoFt! XD

Saludos!

23/3/09 2:37 PM

Haj dijo...

Buena entrevista. Saludos A Don Maligno.

Por cierto y en otro tema, ¿Conoces alguna documentación "al callo" para entender como funcionan las arquitecturas P2P?

Haj.-

23/3/09 3:43 PM

Chen dijo...

Muy buena la entrevista. Un gustazo, sí señor.

23/3/09 4:00 PM

RoMaNSoFt dijo...

Gracias a todos, chic@s (la @ va por d@b!!! jejeje). Venga, ahora en serio, sabeis que os aprecio y a dabito el primero! :*

Uf, uf, menuda aparición... en estos comentarios hay alguien que guarda relación directa con la polémica del Boinas! :-#

-r

23/3/09 6:43 PM

Anónimo dijo...

@RoMaNSoFt: ¿Qué pasó con el Boinas? ¿Qué polémica hubo?

23/3/09 8:30 PM

silverhack dijo...

Eso de pequeña (gran) ciudad me ha encantado....
Eres un máquina. Un honor haberte conocido en persona titi!

23/3/09 9:20 PM

Kuu dijo...

Muy buena la entrevista y gracias por la pregunta 16, ya sé por donde podré empezar (de momento me centro en la carrera, pero este veranito puede ser un buen momento para investigar)

23/3/09 9:32 PM

Anónimo dijo...

Offtopic: espero que algún día comentes esto en tu blog http://lifehacker.com/5177709/chrome-the-only-browser-standing-in-pwn2own-contest

24/3/09 12:31 AM

tayoken dijo...

@Roman: Yo estuve en los dos boinas (el tercero ni lo cuento) y no recuerdo ninguna polémica, bueno, al menos nada que se saliese de lo normal... A parte de que podrían haber dado como ganador a Uri en el boinas 2... Pero vamos, que no creo que el vencedor ganase de manera injusta.

Y del uno... mmm... no sé, creo que también Mandingo fue el justo vencedor.

Quizá me falta información...

24/3/09 2:09 AM

RoMaNSoFt dijo...

@tayoken: son pequeños detalles/anécdotas que a veces se magnifican. De verdad, mejor pasar página, no merece la pena :)

-r

24/3/09 9:47 AM

LordHASH dijo...

Bueno, y como llevais esto de que sea teleco?

Paz!!!
Me parece un crack...

24/3/09 10:29 PM

David Caballero dijo...

Muchas gracias a los dos por esta entrevista. De lo mejor que he leído en mucho tiempo.

7/4/09 10:03 AM

Publicar un comentario en la entrada

Entrada más reciente Página principal Entrada antigua

Suscribirse a: Enviar comentarios (Atom)