ENTREVISTAS: ROMÁN MEDINA-HEIGL HERNÁNDEZ. ROMANSOFT.

Vie, 10/12/2010 - 00:46

Siguiendo con la serie de entrevistas que estamos publicando vamos a publicar la entrevista realizada a RomanSoft otro de los que podriamos llamar nuestros idolos en el mundo de la seguridad :).

Habiamos pensado hacerle una entrevista de ida y vuelta en la que se hicieran preguntas y respuestas pero consideramos que no ha sido necesario. Este hombre contesta todo!. Esperamos que os guste y disfruteis tanto como lo hemos hecho nosotros.

ROMANSOFT. BIO.

Román Medina-Heigl Hernández como nos cuenta en su web es Ingeniero de Telecomunicación por la Universidad de Sevilla, y experto en seguridad informática, campo en el que cuenta con más de 15 años de experiencia y la acreditación CISSP (Certified Information Systems Security Professional).

Son muy recomendables todos sus papers y soluciones que recomendamos leer para aprender sobre seguridad e ingeniería inversa. Le encantan los CTF y ha organizado alguno.

LOS INICIOS:

Empezaste estudiando Ingeniería de Telecomunicación pero tu carrera se ha enfocado sobretodo en el mundo de la informática. ¿Por qué elegiste Teleco y no algo como Ingeniería Informática?

Sinceramente porque en aquel momento (1993) ví con más salidas y mejor valorada la carrera de Teleco. Por otro lado pensé que de Informática "sabía ya muchas cosas" y de Teleco no tenía ni idea por lo que suponía un mayor reto para mí. Además, dado el enorme intrusismo laboral que reina (y reinaba) en Informática, sabía que me podría dedicar perfectamente a la informática (mi pasión), aún habiendo estudiado Teleco. Pensé que mataría dos pájaros de un tiro.

Hoy en día todavía me planteo si acerté o no. Más que nada porque Teleco, al menos en mi época y Universidad -Sevilla-, era inmensamente más difícil que Informática y me supuso un gran esfuerzo. Por otro lado creo que habría disfrutado mucho más la carrera de Informática y le habría sacado más jugo.

Laboralmente hablando hoy le sigo viendo alguna ventaja más a Teleco que a Informática pero también he comprobado que lo que realmente suelen mirar las empresas es si eres "Ingeniero Superior" (da igual si eres Teleco o Informático).

Perdón si he levantado ampollas con el tema Teleco vs Informática, no era mi intención. Simplemente he contestado como lo siento o al menos sentí en aquel momento...

¿Crees que Ing.Teleco te ha abierto alguna puerta en el mundo de la seguridad? ¿Qué te llevó a interesarte por este mundillo de la seguridad?

Básicamente la curiosidad. Desde pequeño siempre me han llamado la atención las "protecciones" (por ejemplo, las protecciones anti-copia que tenían algunas pelis de video, videojuegos, programas...) y cómo saltárselas. O simplemente cómo hacer las cosas "de otra manera". Por ejemplo, ¿a qué tú no has enviado cartas con un sello de 1 pta (cuando su coste real era 20 ptas) o has reutilizado los *mismos* sellos una y otra vez para enviar paquetes gratis? ¿O has jugado a las máquinas recreativas por el módico precio de 1 pta cada 4 partidas (realmente valía 100)? Todo esto sin contar los múltiples trucos de las ya cada vez más obsoletas cabinas de Telefónica, números 900, etc.

Vale, alguno estará pensando que de ahí a dedicarme a la seguridad hay un trecho. Y tiene razón. Así que os sigo contando...

Para ello, nos situaremos en el año 1993: mi primer año de carrera. Por aquel entonces era un fanático del Commodore Amiga y estaba muy metido en la scene española. Era "coder" de un conocido grupo y me manejaba bastante bien en 68k (asm). Siempre me habían llamado mucho la atención las "intros"/"cracktros"/etc y me entretenía destripando muchas de ellas. Colaboraba con una ezine a nivel nacional llamada "Fanzine" relacionaba con el mundo del Amiga pero en el que también aparecían artículos misceláneos. Recuerdo que en uno de sus números aparecieron varios artículos relacionados con las BBS,

el blue-boxing y el hacking en Unix/VMS. Me quedé fascinado y "tocado". A todo esto se unió el hecho de que recién llegado a la Universidad comencé a tomar contacto con una preciosa "sala de terminales" (VT100, etc) que no se parecían nada a un PC o al Amiga. Era todo muy extraño pero muy divertido. Tocado y hundido :-)

Conseguí mi primera cuenta de Unix al poco tiempo (me la prestó un compañero de un curso superior, nosotros todavía no teníamos derecho a ella). También me prestaron un libro gordo cuya portaba rezaba: "Unix System V" (Rosen et al). Era alucinante: un sistema multiusuario, permisos, privilegios, etc. Lo primero que pensé: "eso se tiene que poder romper".

En este caso, la Universidad sirvió para despertar mis inquietudes y por qué no decirlo, disponer de recursos que no tenía en casa. En mi casa no tenía redes de ordenadores ni Internet; y el teléfono era caro (impensable para mí poner un modem). En la Universidad los recursos accesibles por un alumno de primero eran mínimos (recuerdo navegar con el Lynx -modo texto- a 100-500 bytes/seg y eso era ya un lujo) pero al menos teníamos algo. El acceso a los grupos de News y al correo electrónico también fue esencial en mis comienzos.

Contestando ya a la primera pregunta, pienso que más allá del propio conocimiento, el perfil de un Teleco presenta comúnmente cualidades muy valoradas en las empresas (tales como disciplina o constancia, por nombrar dos de ellas). En este sentido sí que se podría decir que es un plus a la hora de conseguir un trabajo. Pero concretamente en el mundo de la seguridad no creo que me haya supuesto una especial ventaja. En mi caso, lo que sí que me ha abierto puertas es ir dándome a conocer a base de publicar algún que otro trabajo e ir relacionándome con personas del "mundillo" vía IRC.

De hecho mi primer trabajo lo conseguí gracias a los dos puntos anteriores, cuando ni siquiera estaba buscándolo. Una empresa tecnológica que estaba comenzando (que llegó a tener unos 100+ empleados) necesitaba un encargado de seguridad: alguien responsable y técnicamente solvente para proteger a la empresa de los hackers (era un negocio puntero -algo así como lo que hoy en día es TomTom- y se esperaban "ataques"). Pensaron que lo mejor era contratar a uno de ellos. Me buscaron y me hicieron una oferta muy pero que muy buena y aunque todavía me quedaban 3 o 4 asignaturas para terminar la carrera acepté la oferta, dejé Sevilla y me vine para Madrid. La empresa nunca tuvo ningún problema de seguridad (más allá de algún virus aislado, algo que es prácticamente inevitable).

He de reconocer que mi caso no deja de ser excepcional: no tenía todavía el título (aún así me contrataron como ingeniero superior) ni experiencia laboral alguna. Pero si me pasó a mí, ¿por qué no te puede pasar a tí?

He visto que tienes CISSP y la Check Point Certification: "CPCS – Pointsec 6.1" en tu currículum, con cual de las dos has aprendido mas? recomendarías alguna? Valoras alguna por encima de cualquier otra? Crees que son necesarias las certificaciones para entrar en este mundo?.

Ambas certificaciones no son comparables. La primera - el CISSP- es genérica (abarca muchos campos y áreas de conocimiento dentro de la Seguridad) y costosa en términos de tiempo de preparación mientras que la otra es una certificación de producto (haces un curso de un par de días sobre un producto concreto, te examinas y listo).

No soy muy amigo de las certificaciones (personalmente no creo demasiado en ellas). Aún así, sí que recomendaría el CISSP puesto que el temario que abarca es amplio e interesante (tiene parte técnica y parte de gestión) y por otro lado las empresas lo valoran bastante bien. Pienso que es "la" certificación en Seguridad. Eso sí, no creo que merezca la pena acumular muchas más certificaciones. Yo sigo leyendo y aprendiendo por mi cuenta (en definitiva, renovándome y mejorando) pero no necesito tener un papel que lo certifique y avale (y que cuesta una pasta, no sólo sacarlo sino también mantenerlo).

Todos hemos tenido algún desliz como blackhat "maloso" cuando hemos sido jóvenes. Cual fue tu primera "hazaña" de la que no te sientas orgulloso en el mundo de la seguridad?

Si te refieres a pifia, que yo recuerde, una muy tonta: renombré el /etc/password de un sistema y justo en ese momento se me cortó el modem. ¡Gluh!

En cuanto a "pequeñas maldades", en los tiempos de oro del IRC he pasado ratos divertidos viendo a gente caer por "ping timeout" ;-). Y hasta aquí puedo leer...

Por lo demás siempre he procurado ser especialmente cuidadoso y cauto en mis incursiones y sobre todo nunca hacer daño a nadie. Nunca he ejercido de "cracker", si es lo que preguntabas, ni he hecho un "rm -rf" para fastidiar a alguien. Mi intención siempre ha sido aprender.

Por supuesto, todo eso ha quedado muy atrás. No merece la pena jugársela y hay muchos campos por explorar y lecciones que aprender sin romper la barrera de la legalidad. Es más, si se sabe aprovechar todo esto... ¡hasta se puede vivir (legalmente) de ello!

Al comenzar en este mundillo, todos tenemos algún ídolo, si tuvieras que elegir, cual seria el tuyo?

En mi época, mucha de la gente que leía en Bugtraq me parecía interesante. Quizás destacar a Alexander Peslyak ("Solar Designer"). Este especialista de seguridad ruso no sólo es el creador de una de las herramientas más usadas en su época ("John the Ripper") sino que además fue pionero en diversas técnicas de exploiting (por ejemplo, el "return-into-libc" base de lo que hoy es el ROP -"return-oriented-programming") así como de defensa (non-exec stack para Linux, Openwall...).

Actualmente "HD Moore" creo que es el que corta el bacalao.

Cuál fue la primera vulnerabilidad que descubriste y a qué edad?

Nunca me he dedicado al bug-hunting "de productos". Siempre me ha gustado más centrarme en aplicaciones "custom" y en construir exploits para vulnerabilidades ya conocidas (por ejemplo, mi exploit para IIS5-webdav llegó a ser muy famoso y hasta aparece referenciado en algún libro).

La primera vulnerabilidad que descubrí y reporté fue un XSS permanente en Squirrelmail. Nada espectacular aunque especialmente grave por dos razones: primero porque este software de webmail estaba muy extendido; y segundo porque te permitía el acceso a algo tan sagrado como el correo electrónico de la víctima. Tenía 29 años.

Cuál es la habilidad que tienes que consideras más importante para ser un buen profesional?

La responsabilidad.

Qué consejos le darías a alguien que quiere buscar un trabajo en el área de seguridad? Como se puede meter la cabeza en un mundo tan hermético?

Entiendo que te refieres a un perfil técnico, ¿verdad? Pues yo para empezar intentaría leer mucho y contactar con gente con similar afición y nivel (siempre es más fácil y ameno aprender en grupo). También abriría un blog técnico para contar lo que vas haciendo, problemas que te encuentras, cómo los solucionas, etc. Con ello consigues dos cosas: que otros puedan aprender de tí (por muy simple que creas que es algo que has escrito, seguro que acaba ayudando a alguien) y también que se puedan fijar en tí (para algún trabajo, etc).

También echaría CV en las empresas de seguridad típicas (ej: s21sec, etc). Siempre hay hueco para alguien que empieza y que muestra interés (y un mínimo de seriedad). Te pagarán 2 duros y serás "operador de" algo pero estarás dentro: comenzarás a conocer gente y podrás aprender de ella. Es una forma de empezar.

Si tuvieras que elegir un país donde desarrollar tu carrera profesional y no fuera España (ni en Repsol YPF), donde seria?

Sin duda, USA.

Y porque USA? Que tiene de especial?

Porque allí un técnico está bien valorado y de hecho, se puede hacer carrera como "técnico" (mientras que en España es inevitable el dar un salto hacia la Gestión, si uno no se quiere quedar estancado laboralmente hablando). En USA es donde están todas las empresas tecnológicas "gordas" y hay más oportunidades.

REPSOL-YPF / GRANDES EMPRESAS

Algunas preguntas sobre Repsol-YPF, si ves que pueden meterte en algún compromiso pasa de ellas.

Por tu experiencia, que te gustan mas las grandes multinacionales o las pequeñas empresas?

No sabría decirte. Lo mejor es que pruebes ambas y decidas por tí mismo :-) Yo he estado en empresas de los dos tipos y cada una tiene sus cosas buenas y malas.

En una empresa grande tienes el problema de "la burocracia": hay muchas áreas, departamentos, procedimientos... es costoso, sobre todo en términos de tiempo -pero también esfuerzo-, conseguir cosas muy simples. Pero por otro lado tienes la oportunidad de cacharrear con trastos caros que probablemente no vas a ver/tocar en una empresa pequeña. Por último, normalmente gozarás de mayor estabilidad laboral.

Yo creo que una empresa pequeña sólo merece la pena si eres tú quien la ha fundado o si te sientes MUY identificado con ella (esto es, tienes algún tipo de lazo que va un poco más allá del meramente salarial). Si no es así te acabarás yendo tarde o temprano.

Que es lo que hace un Ingeniero de seguridad de la información en una gran empresa como puede ser Repsol-YPF, Informática el Corte Inglés o Telefónica Móviles?

Pues muchas cosas :-) Resumiendo: desde labores más técnicas (auditorías y tests de intrusión, evaluación de herramientas de seguridad, análisis y diseño de soluciones de seguridad, desarrollos varios, etc) a las no-tan-técnicas (gestión de proyectos, nuevas propuestas e ideas, análisis de requisitos, escribir RFPs, evaluarlos, etc). Ser polivalente es una cualidad muy importante en un perfil.

UOC

Que te aporta ser profesor en la UOC, y como acabaste siéndolo?

Me convenció mi amigo Chema Alonso (los que lo conocen saben que es un "liante" de cuidado; y los que me conocen a mí saben que me dejo -¿dejaba?- liar con cierta facilidad). Yo nunca antes me había dedicado profesionalmente a la docencia y pensé que sería interesante la experiencia.

Cuales son las carencias como profesor de la uoc?, Sufriste el XSS del correo?

Aunque quede feo decirlo pero... creo que no está bien pagado. En mi caso, además tuve ciertos pequeños líos con Administración (que me costaron mi tiempo). La plataforma de e-learning a veces estaba caída. Y sobre todo, eché de menos que la cuenta de @uoc.edu no estuviera accesible vía IMAPS/SSMTP.

Respecto al XSS seguro que alguien tiene mi cookie de sesión por ahí... ;-)

PAPERS Y WEB(RS-LABS.COM)

Qué blog te da más rabia? y Cual es tu preferido?

Uno que me de rabia en especial no te sabría decir. En general aquellos que no son originales sino que se dedican a copiar y pegar noticias de allí y de allá. Prefiero leer la fuente.

Preferidos tengo muchos y los tengo ordenados por apartados... Por ejemplo, tengo un apartado que me gusta especialmente llamado "CTF" donde recojo aquellos donde se publican soluciones a challenges. Son muy técnicos y se puede aprender trucos de ellos (por ej, blog.nibbles.fr y blog.stalkr.net). En el apartado "Seguridad Españoles" resaltar a blog.48bits.com, www.pentester.es y www.elladodelmal.com. En el apartado "Seguridad" a secas tengo los típicos: metasploit, skypher.com, etc.

Últimamente no tengo mucho tiempo para leer blogs y lo que hago es ver sólo algunas entradas cuyos enlaces publica la gente vía Twitter (tienes la ventaja de poder ver quién lo recomienda y esto a veces te

chidos publica la gente via Twitter (tienes la ventaja de poder ver quien lo recomienda y esto a veces te sirve para saber por adelantado -sin verlo- si la entrada merecerá la pena o no).

Estas al tanto de la noticia que apareció hace unos días sobre el modo DEBUG en los procesadores AMD. Que crees que puede suponer para un reverser este descubrimiento? (http://www.woodmann.com/collaborative/knowledge/index.php/Super-secret_d...!)

Algo leí pero un poco por encima. No parece que afecte a la seguridad (para tener acceso a la "nueva" funcionalidad hay que tener privilegios), con eso me quedo tranquilo :-) Como mucho, se podrá aprovechar para mejorar algún debugger aunque sinceramente tampoco lo veo muy necesario.

Los rumores dicen que tu web la programas con vi, joe e incluso emacs, puedes confirmar los rumores? Para cuando un re-estiling mas 2.0?

Soy hombre de "vim" (y en mis viejos tiempos de "jed") pero normalmente utilizo UltraEdit desde Windows para actualizar mi web. En cualquier caso, siempre edito el HTML a pelo. Es un atraso, lo se...

Alguna vez he pensado en remodelar mi site pero no me gusta mucho el "diseño web" y me da una pereza horrible ponerme así que lo voy dejando y dejando... Además, ¿no está bien como está? Lo que importa es el contenido :-)

Y por cierto, desde que tengo twitter (@roman_soft) ya soy un hombre 2.0, ¿o no?

¿En la entrevista que le hicimos a Chema Alonso de http://www.elladodelmal.com/ nos dijo que tu habías sido uno de sus ídolos, que se siente siendo el ejemplo a seguir de personas como Chema Alonso?

A todos nos gusta que se nos reconozca nuestro trabajo. Yo no soy la excepción ;-). En este caso, para mí se trata de un halago puesto que además de buen amigo, Chema es un gran comunicador y profesional de la seguridad. Es ameno, divertido y sabe cómo tratar a la gente. Yo también le admiro.

HOBBIES

Para terminar, cuéntanos algo sobre tus Hobbies:

Qué prefieres unos billares y cervezas o salir de marcha a quemar la noche? Billar o futbolín?

En general, las cervezas (pero si se demoran hasta altas horas de la madrugada con alguna copa de por medio tampoco le hago ascos :-)). Respecto a lo segundo, futbolín a muerte (pero de los "de verdad", es decir, los de hierro con jugadores de "2 patas").

Si fueras tu el que se está haciendo esta entrevista, que es lo que crees que se te ha olvidado preguntarte y no debieras de pasar por alto?

Es raro que no me hayas preguntado por mi afición a los wargames (CTFs, etc). Ni tampoco por otro tema que ha sonado mucho este año (que casi prefiero obviar así que no voy a darte ninguna pista :-P). Ah se me olvidaba tampoco me has preguntado por !dSR.

Cierto, cuando vi tu respuesta me di cuenta que se me habia pasado los wargames!

Participaras en el ctf ructfe 2010?

Sí, estaré ahí pero de incógnito. "Int3pids" no participa oficialmente. Un CTF (de tipo attack&defense) requiere de mucha preparación previa y un cierto rodaje, si se quiere tener alguna posibilidad. En nuestro caso, aunque todos tenemos mucha experiencia en wargames de diferentes estilos, nuestro equipo actual es joven y es el primer CTF que abordaremos juntos por lo que nos lo pensamos tomar con calma y utilizarlo como calentamiento. Eso no quiere decir que no vayamos a dar caña (es una técnica para que nuestros oponentes se confíen y bajen la guardia :-)).

!dSR? Qué es!??. Reconozco que me has pillado. Tienes algo que ver con eso?. Cuentame que es. Sigue existiendo como grupo/organización/hacklab o lo que quiera que sea?

!dSR (http://www.digitalsec.net/) comenzó como un grupo de amigos (<10 personas) que compartíamos interés por la seguridad informática en general y el hacking/pen-testing en particular. No había ninguna directriz comogrupo sino que cada cual publicaba o hacía y deshacía a su antojo. Quiero decir, que algunos miembros son/somos "supporters" del "full-disclosure" y otros no lo son tanto; y también que algunas acciones que aparecen firmadas como grupo no tienen por qué contar con el beneplácito de todos sus miembros (ni siquiera de su mayoría).

Entre sus hazañas una bastante sonada fue el hackeo al mítico CCC (Chaos Computer Club) alemán, en Noviembre de 2004, obteniendo datos (user, pass, email, ...) de todos los registrados/asistentes a uno de sus Camps (una especie de meeting/congreso de seguridad): http://www.digitalsec.net/stuff/fun/CCC/ccc_and_cccs.txt. Como anécdota, contar que el hackeo fue posible gracias a una vulnerabilidad 0day que yo mismo encontré (en Twiki) y cuyo exploit desarrollé (¡pero yo no tuve nada que ver con la intrusión en sí!). Otra cosa que me llamó mucho la atención y me sorprendió (gratamente) es la deportividad con la que se lo tomó la gente del CCC: el mismísimo Harald "laforge" Welte nos envió un mail que comenzaba así: "First I'd like to congratulate you on behalf of the CCC Berlin e.V. to opening our TWiki on blackhole" (http://www.digitalsec.net/stuff/fun/CCC/note.txt). También estuvimos en contacto con otros miembros de la cúpula del CCC y he de decir que el trato siempre fue bueno. Bueno, sólo hubo un pequeño detalle... una persona al parecer del CCC (pero sin el apoyo/consentimiento del mismo) hizo pública mi vulnerabilidad/exploit sin dar los créditos correspondientes. Y yo se la lié parda. Puedes leer algo más sobre el tema en: http://www.rs-labs.com/noticias/#12

Actualmente !dSR como grupo está inactivo (desde hace años). Pero en su lugar y en torno a él (en paralelo) fue creciendo toda una Comunidad compuesta no sólo por los integrantes originales del grupo sino también por amigos, conocidos, que en general, son los que cortan hoy día el bacalao de la seguridad en España. Actualmente la comunidad !dSR tiene 80 miembros. Se trata de un foro técnico y privado, que yo co-administro, por lo que el acceso no está abierto al público (de hecho, actualmente no se aceptan nuevos miembros).

En que canal sueles estar en el irc? (y en que red?)

Hace años que me desintoxiqué del IRC. Ahora apenas entro, a no ser que haya algún "evento" especial (algún concurso, CTF, wargame, etc). También me gusta entrar de vez en cuando a saludar a mis amigos de 48bits.com.

una pregunta mas.. qué listas sigues de seguridad? cómo te mantienes informado?

Estoy apuntado a bastantes listas públicas pero las que procuro seguir siempre son: bugtraq (securityfocus), full-disclosure y daily-dave. Para mantenerme informado, aparte de las listas públicas, sigo listas privadas (como !dSR), muchos blogs y dedico también bastante tiempo a leer mi twitter (@roman_soft).

Mención especial a Alex(http://dnieyfirmadigital.blogspot.com/) compañero mio de la UOC que me ha ayudado a pensar las preguntas.

Versión para impresión | *Enviar a un amigo*

COMENTARIOS

ENVIAR UN COMENTARIO NUEVO

Asunto:

Comentario: *

Las direcciones de las páginas web y las de correo se convierten en enlaces automáticamente.
Etiquetas HTML permitidas: <a>   <cite> <code>   <dl> <dt> <dd>
Saltos automáticos de líneas y de párrafos.

Más información sobre opciones de formato

CAPTCHA
This question is for testing whether you are a human visitor and to prevent automated spam submissions.

What code is in the image?: *

Enter the characters shown in the image.

Vista previa