



## ROMÁN MEDINA-HEIGL HERNÁNDEZ

Correo electrónico: [roman@rs-labs.com](mailto:roman@rs-labs.com)

### DATOS PERSONALES

---

*Domicilio Habitual:*

\*\*\*\*\*

28022 – Madrid

Nacionalidad: Español

Servicio Militar: Exento

Estado Civil: Casado

Fecha Nacimiento: 1975

### CONOCIMIENTOS

---

- *Programación:* C, Asm (68k, x86), Shell (Bash), HTML, JavaScript, PHP, Perl, SQL, Basic.
- *Sistemas:* Linux (Debian, SuSE, RedHat, Fedora, Ubuntu), Solaris, Tru64, Cisco IOS, MS-  
{DOS, Windows 9x / NT / 2k / XP / 2k3}, Amiga OS.
- *Bases de Datos:* Oracle, MySQL, PostgreSQL, Microsoft SQL Server, SQLite.
- *Redes:* Sólidos conocimientos de redes y protocolos basados en TCP/IP, Programación Unix; QoS, Ethernet, Wireless. Routers ADSL y RDSI ; Switches, Hubs. PoP. VPN. Arquitectura LDAP. Proxies. *Experiencia en Internet desde 1994.*
- *Seguridad:* Criptografía, Cortafuegos, Proxies inversos, Pen-Testing - Hacking ético, Análisis de Vulnerabilidades y Desarrollo de Exploits, Hardening, Análisis forense, IDS / IPS, Gestión de Identidades (IM), WiFi, Alta Disponibilidad y Balanceo de carga. Filtrado de Contenidos. Antispam. *Experiencia demostrable: 15 años.*
- *Aplicaciones:* Office 97/2000/XP/2003, Spice, Matlab, VMware. Diseño web.
- *Idiomas:* Español (nativo). Inglés técnico nivel alto leído y escrito. Conocimientos de Alemán.

### FORMACIÓN

---

- Titulación en *Ingeniería de Telecomunicación*, especialidad *Telemática*. Escuela Superior de Ingenieros, Universidad de Sevilla.
- Proyecto Fin de Carrera titulado “Análisis de seguridad, optimización y mejora de un portal web basado en PHP y MySQL”, evaluado con la calificación de “Sobresaliente – 10”. Comprende aspectos de ingeniería de software y seguridad informática.
- Acreditación CISSP (Certified Information Systems Security Professional). (ISC)<sup>2</sup>. Diciembre 2006.
- Curso "Sun ONE Directory Proxy Server". Sun Microsystems. Abril 2004.
- Curso "IPv6". Eurocomercial I&C. Junio 2004.
- Curso de Administración de Oracle. AFI, S.L. Noviembre 2004.
- Certificación Check Point: “CPCS – Pointsec 6.1” (End-point security). Junio 2008.
- Curso “Dirección de Proyectos: Proyectos Informáticos” (PMAsores, 28 PDU’s). Octubre 2010.
- Skybox Certified Assurance Engineer (SCAE). Skybox Security. Diciembre 2010.
- Skybox Certified Risk Management Engineer (SCRE). Skybox Security. Diciembre 2010.
- Certificación “Fundamentos ITIL v3”. APMG-International. Julio 2011.
- Curso “R7522TES – IBM Security Site Protector System Basic Implementation and Administration Workshop”. IBM Servicios de Formación. Diciembre 2011.
- Curso “R7521TES - IBM Security Network Intrusion Prevention System (IPS) Configuration and Deployment Workshop”. IBM Servicios de Formación. Diciembre 2011.

### EXPERIENCIA PROFESIONAL

---

Sep/2010 – Actual

Repsol YPF, S.A.

INGENIERO DE SEGURIDAD DE LA INFORMACIÓN.

- En el área de “Ingeniería de Seguridad” se forjan nuevos proyectos, se prueban productos punteros y se diseñan arquitecturas seguras. Funciones:
  - Innovación. Proponer proyectos e ideas que supongan una mejora sustancial de la seguridad.

- Gestión de proyectos de seguridad y los recursos asociados.
- Apoyo técnico como especialista de seguridad.
- Responsable del grupo de Antivirus y Vulnerabilidades.
- Análisis forense.

Jun/2007 – Ago/2010 IECISA (Informática El Corte Inglés, S.A.)

ARQUITECTO / CONSULTOR DE SEGURIDAD INFORMÁTICA.

- En el “CEX (Centro Experto) de Telecomunicaciones, Seguridad e Ingeniería C4I”, participando en diferentes proyectos:
  - Auditorías de seguridad y tests de intrusión en sectores público y privado (ej: Ministerio de Defensa, Unión Fenosa, etc).
  - Consultoría y Diseño de la Arquitectura de Seguridad del sistema de Tele-Gestión en Baja Tensión de Endesa.
  - Seguridad del puesto de trabajo (“End-point security”): autenticación / cifrado de dispositivos USB, discos duros, etc. Tecnologías: Pointsec (Check Point) y Zitralia.
  - Soluciones de firma electrónica, protección de datos e identidad digital. Infraestructura de Clave Pública (PKI). Tecnologías: Safelayer.
  - Análisis de vulnerabilidades en aplicaciones web, proxies de navegación web segura así como otros proyectos para el grupo de Ingeniería de Seguridad de Repsol.

Mar/2010 – Actual UOC (Universitat Oberta de Catalunya)

PROFESOR CONSULTOR DEL MASTER DE SEGURIDAD INFORMÁTICA.

- Impartiendo la asignatura de “Seguridad en Sistemas Operativos”.

Feb/2004 – May/2007 Telefónica Móviles España (a través de AFI, S.L.)

JEFE DE PROYECTO / INGENIERO DE SEGURIDAD INFORMÁTICA.

- En el departamento de Seguridad del área de Red de TME (“Gerencia de Seguridad de Redes y Servicios”), trabajando en los campos de I+D, consultoría y gestión de proyectos. Proyectos realizados de forma íntegra:
  - Desarrollo, implantación y operación del “área de análisis y comunicación de amenazas” (dentro del marco de la Gestión de Seguridad Operacional).
  - Diseño e implementación de un proxy inverso “avanzado” (posteriormente publicado en SourceForge con licencia GNU).
  - Plataforma de autenticación (TACACS+, Radius, LDAP, Proxy LDAP, etc.) y gestión de identidades.
  - Alta disponibilidad por software (VRRP en Linux, Heartbeat / Mon en Solaris).
  - Diseño e implementación de un Proxy SNMP (Linux / Netfilter / Iptables).
  - Análisis de herramientas software de auditoría de seguridad. Evaluación de hardware de seguridad.
  - Gestión de usuarios (Metadirectorio / Novell DirXML).
  - Evaluación, modificación e implantación de un Proxy FTP “open-source” sobre Linux (jftpgw).
  - Evaluación y depuración de un Proxy LDAP (SunONE).

May/2003 – Feb/2004 Optenet, S.A.

COORDINADOR DEL ÁREA DE SISTEMAS / INGENIERO DE SISTEMAS.

- Responsable de área. Planificación de instalaciones.
- Integración de la tecnología líder en selección y filtrado de accesos a Internet desarrollada por Optenet sobre diferentes arquitecturas (sistemas Solaris, Linux, AIX, Novell, Windows y appliances como NetApp NetCache, BlueCoat y Cisco PIX) en entornos del cliente y diferentes ámbitos: usuario final, servidor e ISP.
- Manejo de proxies: Squid, MS Proxy, ISA Server, Novell Border Manager.
- Participación en el programa de beta-testing oficial de Cisco realizando pruebas del protocolo ICAP sobre la futura versión 5.1 del “Application and Content Networking System Software (ACNS)” para Cisco Content Engine.
- Soporte técnico (help desk) de último nivel.

- Sep/2002 – Dic/2002 Ubeda Virtual, S.L.  
CONSULTOR DE SEGURIDAD Y NUEVAS TECNOLOGÍAS.
- Elaboración de soluciones a medida y planes de mejora de infraestructura: redes, seguridad e Internet.
- Oct/2000 – Jul/2002 Batmap, S.A.  
RESPONSABLE DE SEGURIDAD / ADMINISTRADOR DE SISTEMAS DE SEGURIDAD.
- Responsable de Seguridad. Desarrollo de políticas de seguridad, configuración de firewalls, VPN, Antivirus, etc.
  - Director del Dpto. de Mantenimiento. Soporte técnico a usuarios, compras de material informático.
  - Administrador de red. Configuración de routers, switches (VLAN, trunking, etc.), balanceadores de carga (Radware WSD).
  - Diseño, instalación, configuración y mantenimiento de la totalidad del PoP (punto de presencia) sito en Madrid y compuesto por diversos servidores con balanceo de carga y alta disponibilidad.
  - Instalación, configuración y mantenimiento de sistemas heterogéneos Unix / Windows. Servidores Unix: Web (Apache), DNS (Bind), Correo (Sendmail / Qpopper), FTP (Proftpd, BSD ftpd), Proxy (Squid), Aplicaciones (Tomcat, Cocoon), Bases de datos (MySQL), E-Commerce (Apache + SSL + PHP), Ficheros SMB (Samba), IRC (Ircu), IDS (Snort). Servidores Windows: IIS, Serv-U.

## PUBLICACIONES

---

Artículos en la revista @rroba:

- “Caso real y práctico de hacking”, Septiembre 2002, nº 60, pp. 84-87.
- “Izhal: una comunidad dedicada al hacking”, Octubre 2002, nº 61, pp. 16-19.
- “Hack21: diario de un participante”, Mayo 2003, nº 68, pp. 16-19.
- “El regreso de los Boinas Negras. Solución al II reto de hacking web”, Noviembre 2003, nº 74, pp. 22-26.

Artículos en formato digital [<http://www.rs-labs.com/papers/>]:

- “Tácticas de guerra en el IRC”, Septiembre 1999.
- “Boinas Negras: una solución al concurso”, Febrero 2003.
- “Solución al reto de análisis forense de RedIRIS”, Diciembre 2003.
- “Solución al III Reto Hacking - El lado del mal”, Mayo 2007.
- “Blind LDAP Injection: Solución al Reto Hacking #4 - El lado del mal”, Septiembre 2007
- “Solución al Reto Hacking #5 - El lado del mal”, Enero 2008.
- “Solución al problema #15 - Codegate 2009 (Prequals)”, Marzo 2009.
- “Solución a la prueba #3 del Reto Panda”, Abril 2009.
- “Solución al Reto Hacking #10 - El lado del mal”, Septiembre, 2009.
- “La historia de Rooted CON”, Mayo, 2010.
- “SbD Wargame 2011 write-up”, Febrero, 2011.
- “Rooted Arena 2012 - Complete write-up”, Marzo, 2012.

Conferencias:

- Microsoft TechNet. “Cómo realizar un test de intrusión a una aplicación web”. 4/Oct/2007. Getafe (Madrid).

Proyectos:

- [RewritingProxyTME](#) – Proxy inverso HTTP. Marzo 2005.

## ACTIVIDADES

---

- **Organizador** del concurso de seguridad: “Web challenges from RootedCON’2010 CTF” (internacional) [Septiembre 2010].
- **Miembro fundador** del Congreso de Seguridad Informática “Rooted CON” (<http://www.rootedcon.es/>) y co-organizador del concurso CTF del mismo [Marzo 2010].

- **Ganador** de los concursos de seguridad informática: “Rooted Arena 2012” (team “int3pids”, nacional) [Febrero 2012], “Swiss Cyber Storm 3 - CarGame Challenge” (team “int3pids”, internacional) [Mayo 2011], “SbD Wargame 2011” (team “int3pids”, internacional) [Enero 2011], “CTF Pre-Ekoparty (5ª edición)” [Agosto 2009] (internacional), “El reto Panda” [Mayo 2009] (nacional) y “Reto conmemorativo del décimo aniversario de “una-al-día” de Hispasec Sistemas” [Noviembre 2008] (nacional). Tercera posición en las “prequals-CTF” de “Codegate 2010” (el segundo concurso internacional más prestigioso del mundo) [Marzo 2010].
- **Participación** en numerosos retos, wargames y concursos relacionados con la seguridad informática. Superados con éxito: Hackerslab, NGSEC’s Game #1 y #2, Boinas Negras #1 y #2, Mod-X, Izhal, Arcanum, Cyberarmy, Hack21 #2, Yoire, Blindsec #1 y todos los retos de Informática64. Participación en el reto de análisis forense de RedIRIS.
- Desarrollo de **exploits** (ej: “IIS 5.0 WebDAV -ntdll.dll-“, “Linux Kernel 2.6.x PRCTL Core Dump Handling”, “ISC DHCPd 2.x DoS”, “Postfix local root”). Descubrimiento e investigación de nuevas **vulnerabilidades** (ej: “SquirrelMail” [BID 10439 / CAN-2004-0520]). **Hacking** de aplicaciones web y defensa (ModSecurity). Automatización de tareas (**scripting**). Diseño, implantación y gestión de un ISP seguro (Hosting y Servicios de Backup Remoto). Programación de intros/demos gráficas en Asm-68k para la Amiga-scene. Conocimientos de **ingeniería inversa** (cracking). Profundo conocimiento del protocolo IRC. Desarrollo de una aplicación de gestión para laboratorio de análisis agrarios (en producción desde hace más de 10 años).

## OTROS DATOS DE INTERÉS

---

Carnet de conducir B1 y A2. Vehículo propio. Capacidad de análisis y documentación. Gestión de equipos/personas. Autodidacta. Web personal dedicada a I+D y Seguridad: <http://www.rs-labs.com>.