Berlín, Crónica del 19 Congreso del Chaos Computer Club

19C3, Out of order

Daniel Fernández Bleda, Pablo Garaizar Sagarminaga, Jorge Gómez Arenas, Marcos Serrano

Después de tres días mezclándonos con la comunidad hacker más antigua y famosa de Europa, todavía tenemos sentimientos encontrados respecto al congreso, donde se pudo ver lo mejor y lo peor de la escena europea.

Lo primero que nos sorprendió fue el ambiente casi soviético de Berlín del Este, y sus calles heladas. A pesar del frío y de lo avanzado de la noche, había gente desde el jueves en la puerta del Haus Am Köllnischen Park, sede del 19c3 (decimonoveno congreso del Chaos Computer Club). El congreso tiene una duración de tres días completos, de viernes a domingo, ambos incluidos.

Al llegar al congreso la primera sorpresa fue la larga hilera de gente esperando para entrar. Acompañados de un frío digno del diciembre centroeuropeo, pagamos nuestro pase para los tres días, un tanto sorprendidos por los precios y por la comercialización del evento (40 € para un pase de tres días, 20 € para los pases diarios). Lo siguiente fue registrar nuestros ordenadores portátiles mediante unas pegatinas numeradas, una para el portátil y otra pegada a la acreditación, de tal forma que para salir se comprueba si el portátil y la acreditación tienen el mismo número.

Nuestra expedición disfrutando de los encantos de Berlín.

La primera impresión (que es la que cuenta) fue muy buena, mucha gente, ordenadores por todas partes, un montón de actividades y muy buena infraestructura. El calendario de charlas que conocíamos había cambiado y era necesario estar atentos a las modificaciones, indicadas mediante carteles o en la página web del congreso. Llamaba la atención la gran cantidad de portátiles que había y la inmensa mayoría con sistemas libres, era raro ver Windows o MacOS en las pantallas LCD. Había varias zonas, 3 para charlas con ponente y proyector (Saal 1, Saal 2 y Saal 3), 1 de talleres (Saal 5), 2 de actividades varias (Lockpicking y Laboratory), un hackcenter, art & beauty, la cafetería "Chaos café" y una zona de relax llamada "Haecksenraum". Como vemos, era difícil aburrirse, mucho más si contamos con la red wireless que envolvía al edificio: un auténtico "Chaos" donde se podía encontrar de todo: repositorios de ISOs de los diversos *BSD's, servidores de FTP con acceso anónimo, sniffers tratando de adivinar la dirección del gateway...

Phenoelit: ¡Tu impresora está escaneando mi red!

Lo primero que hicimos fue intentar buscar una charla interesante, después de darnos cuenta de que la charla de las 11:00, "Mastering Regular Expressions", que impartía uno de los compañeros que venía con nosotros ya había terminado. El CCC (Chaos Computer Club) había anunciado que tenía la intención de alejar el congreso del oscurantismo de la escena hacker alemana. El primer esfuerzo en este sentido ha sido intentar aumentar el número de charlas en inglés en el congreso. Desde el punto de vista de alguien que no habla ni una palabra de alemán (como nosotros), la intención ha sido buena, aunque no siempre se han cumplido las expectativas.

Deambulamos un tiempo entre la cafetería y el Hackcenter, donde sólo tenían cabida los ordenadores registrados. La mañana del viernes tenía charlas interesantes, aunque no todas eran en inglés: TCP/IP para principiantes, Perl, segundad en redes wireless, TCP/IP v6, Ataques a sistemas de red embebidos... Asistimos a estas dos últimas, la primera de ellas impartida por un desarrollador del proyecto Netfilter, Harald Welte, que dio una visión general de la nueva versión del protocolo IP. Inicialmente preguntó si los asistentes preferían la charla en inglés o en alemán, nuestras voces no fueron oídas y la charla fue finalmente en alemán. La siguiente charla, "Attacking networked embedded systems", fue impartida por dos integrantes del grupo Phenoelit y se ajustó a la idea que teníamos de lo que era una charla en el CCC: muchísima calidad técnica, explicaciones

detalladas y muy divertidas, herramientas propias puestas a disposición del público y un campo relativamente novedoso. Nos explicaron cómo montar servidores de ficheros, servidores web que crackean contraseñas, escaneos de redes, etc., todo ello desde impresoras HP, modificando el soporte para java que proporcionan las impresoras de gama alta. Fue muy divertido el enfoque que dieron a la charla, todo el rato haciendo bromas ("¡Ey! ¡¡tu impresora está escaneando mi servidor!!") y detallando sus investigaciones con programas propios.

A las 16:00 comenzaba la charla sobre TCPA, el mecanismo de control mediante hardware que quieren imponernos a partir de 2008, y tras dos horas de exposició, se reservó otra hora en otro recinto improvisado para debatir acerca de ese espinoso tema. Mientras tanto, en la sala 2 asistíamos a una charla sobre "TCP state/window tracking + stat", por Harald Welte, el mismo ponente que horas antes nos habló sobre TCP/IP v6. Welte explicó detalladamente las dificultades que entraña hacer un seguimiento de los diferentes estados de las conexiones TCP, con numerosos ejemplos sobre condiciones extremas y los problemas derivados. Fue una charla interesante, aunque quizá 60 minutos fueran pocos para hablar de todo aquello.

Ya para entonces nos habíamos recorrido todo el edificio. La visita al recinto de "Art & beauty" fue ¡mpactante, ambiente oscuro, vídeos proyectados en las paredes, ordenadores, diseño contemporáneo, etc. El "Haecksenraum" lo hicieron aprovechando un descansillo en el piso de arriba, donde había puestos fijos con ordenadores conectados a Internet, sillones, sofás y enchufes para los portátiles, que fue sin lugar a dudas el don más preciado de todo el congreso, era fácil ver varios alargadores conectados entre sí para que las baterías no pudieran estropear la velada.

A media tarde asistimos a la charla "A GNU approach to improving Unix security", en la que se describió la nueva visión en cuanto a seguridad que ofrece el sistema GNU/Hurd. La impartieron dos hackers del propio proyecto, que explicaron los métodos de autentificación y las características asociadas a la gestión interna del sistema (varios servidores intercambiando mensajes en lugar de un kernel monolítico que controle el sistema). El momento estelar de la charla fue al principio, cuando uno de los ponentes entonó la famosa canción "join us and share the software, you'll be free hacker, you'll be free", una experiencia que no se ve todos los días y relata perfectamente el ambiente que se vivía.

*El **Haecksenraum,** portátiles con tarjetas wireless al ritmo de la música drum&bass.*

La caravana hacker, un autobús remodelado con LAN wireless, portátiles, y camas, el paraíso móvil

El día lo cerraban charlas sobre la retención de datos en la Unión Europea, el Proyecto Ada Lovelace, un taller sobre IPSec y un coloquio sobre el propio CCC, todo ello en alemán. A última hora en la sala 1, asistimos a la presentación de un vídeo que relataba varias "performances" de un grupo activista ruso en las calles de Moscú, donde nos llamó especialmente la atención las manifestaciones forzadas por 2-3 personas con técnicas muy oportunistas.

Un pingüino en mi X-box

El segundo día del congreso amaneció con una charla sobre NetBSD para sistemas embebidos. A lo largo de la mañana se sucedieron varias charlas en alemán acerca de temas bastante variopintos: RSA, AES Attacks, DNS, .net, IPv4-IPv6 o análisis del control de flujo de programas para malware. Esta última charla vino de la mano del conocido grupo Teso, que explicaron en profundidad sus herramientas de ingeniería inversa, generando grafos con el flujo de ejecución de los programas investigados y mucha información acerca de los mismos. A pesar de ser en alemán, mostraron código en C y screenshots de sus programas. Después de comer asistimos a la charla "Lawful Interception of IP Traffic: The European Context", por Jaya Baloo, donde se explicó las medidas que adoptan los gobiernos para capturar el tráfico IP que circula por sus redes mediante diversos métodos. Un auténtico terror para paranoicos. Mientras tanto, la parte BSDera de nuestra expedición asistió a "Clustering the NetBSD Operating System for Video Rendering", un título muy prometedor para una charla que decepcionó. De tecnología de clustering no hubo más que el nombre de la charla ya que todo se basó en unos cuantos scripts que repartían el trabajo en fragmentos y varias máquinas con xload ejecutando cada uno de los trabajos. El sistema repartía el fichero grande entre varias máquinas por NFS, cada una trabajaba sin colaboración, y posteriormente desde el "nodo central" se comprobaba que había finalizado todo correctamente y se unían las partes. El conjunto de

Un auténtico Chaos organizado

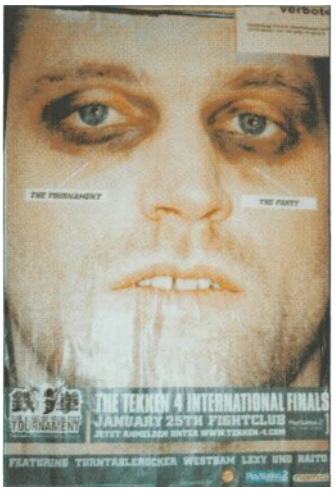
Zero Hacking Tool en la Sala 1, por Nils Magnus.

utilidades que emplearon hace que su experiencia no sea extrapolable para otro tipo de trabajo distribuido por lo que al salir de la sala queda la impresión de que lo explicado no ha valido para nada.

El desencanto anterior lo rompió la magnifica charla "Itts my box: how the hardware and software traps in the Xbox were beaten and Linux installed" en la que el equipo de X-BoX Linux (Andy Green, Milosoch Merlac, Michael Steil y Frand Lehner) nos demostró cómo la filosofía, basada en el dinero como único medio y objetivo, que tiene Microsoft no tiene comparación con la tenacidad de aquellos investigadores cuyo único fin es el de abrir los sistemas a todo el mundo. Cuando la casa de Redmond apostó por las consolas e invirtió una cantidad indecente de dinero de su proyecto X-Box en seguridad jamás pensó que el "virus" llamado Linux tendría una opción en el menú de arranque de su consola. Todos los integrantes del equipo fueron detallando cada uno de los pasos seguidos para ir superando cada una de las trampas que iba poniendo Microsoft en su camino, siempre dentro de la estricta legalidad. Hardware, programación a bajo nivel, criptografía y un finísimo sentido del humor hicieron de esas dos horas una auténtica delicia. Al final de la charla pudimos ver cómo la consola verde y negra es capaz de ejecutar un fantástico Linux Mandrake funcionando al 100% y cómo Tux se adueñaba de la imagen de inicio, añadiendo color a una pantalla "demasiado apagada".

La red wireless envolvía el edificio

Al terminar el día escuchamos dos charlas más: "Detecting DDos Attacks and Countermeasures at ISPs" y "SCTP (Stream Control Transmission Protocol)", ambas demasiado teóricas, más cercanas de un aula universitaria que de un congreso del CCC. Mientras tanto, en la sala 1 tenía lugar una "Patent Party", donde se ridiculizaban a las patentes de software con una función pseudoteatral acompañada de piano. A última hora descubrimos los proyectos del "Laboratory", con las blinkenlights (rememorando la famosa construcción de dibujos con las luces de oficina en un edificio berlinés), los talleres de antenas wireless, robótica con LEGO, radiofrecuencia, música, etc.



Cartel promocional del campeonato internacional de Tekken 4.

Lock-picking, seguridad física poco hortodoxa

Por la mañana del tercer y último día nos levantamos con un jarro de agua fría. De las mismísmas honduras del pensamiento surgió Nils Magnus. Disfrazado de Neo y sin quitarse en ningún momento sus gafas de sol, nos "deleitó" con "Zero Hacking Tool": cómo hackear una red con las herramientas básicas de Unix. Con este aparatoso título nos enseñaba a conseguir una ip libre dentro de una red sin utilizar dhcp, calcular máscaras, encontrar el gateway y hacer un mapeado de la red. De esta charla nos quedamos con una joya: alguien entre el público preguntó de qué forma mágica había conseguido hallar el gateway de la red, ante lo cual, y sin ningún reparo, el ponente respondió que éste suele localizarse en la primera dirección IP del rango. ¿Cómo es posible que en un congreso del CCC alguien suelte eso sin caérsele la cara de vergüenza? Para olvidar. Este enfado inicial se fue calmando después de asistir a "How to find anything on the web", donde "fravia" nos contó pequeños trucos para optimizar nuestras búsquedas en Internet. La charla no tuvo nada underground, pero fue bastante amena y graciosa por momentos.

A las 13:00, los organizadores del taller de "Lock picking" hicieron una sesión en castellano, donde coincidimos con varios miembros de Hispahack mientras tratábamos de reventar cerraduras juntando las técnicas recién aprendidas y nuestra poca maña.

La última charla que escuchamos fue "Spam Prevention", por Stefan Seis, en la que se analizaron los diferentes sistemas existentes para prevenir el spam. Fue una charla concisa y breve, pero en el turno de preguntas se produjo un interesante y acalorado debate sobre el tema, que añadió emoción a la sala.

Mientras los germanoparlantes se morían de risa con el "Beopardy - The Hacker Jeopardy", nos reunimos en el "Chaos Café" para hablar de todo lo pasado en estos tres intensos días, y precisamente esa charla es lo que has podido leer. La conclusión que podemos sacar es que el congreso del CCC es un evento consolidado y serio, con algunas ponencias que no han llegado a lo esperado y otras que han sido geniales, múltiples zonas distintas donde hacerte "tu propio CCC congress" y un elenco de hackers con ganas de divertirse. A

*No todo fue **CCC,** la puerta de Brandemburgo, visita obligada en Berlín.*

Referencias

- 19 Congreso CCC: https://www.ccc.de/congress/2002/index.en.html
- Phenoelit: http://www.phenoelit.de
- Hispahack: http://hispahack.ccc.de