
The Security Sentinel

**The Security Sentinel (TSS) es una compañía española dedicada a al seguridad informática,** tan olvidada por muchos y tan importante. TSS se dedica a realizar auditorías de seguridad a empresas, basándose en el hacking ético o pruebas de pentesting, además de impartir cursos de formación sobre seguridad.

El malware y las vulnerabilidades son un tema de actualidad en nuestro blog y sobre todo con las últimas noticias sobre VENOM, Heartbleed, y otros problemas de seguridad que afectan a GNU Linux. Por eso hemos decidido entrevistar a **Francisco Sanz, el CEO de TSS** que nos dará algunas claves sobre este interesante tema.

**Francisco (FS a partir de ahora) es uno de los profesionales de TSS**. Él cursó ingeniería informática en la Universidad Autónoma de Madrid para luego licenciarse en gestión comercial y marketing en la ESIC, realizar el CNNA de Cisco, cursos de programación PHP y MySQL, hacking ético y conseguir superar el certificado CEH de EC-Council con una clasificación del 91%/100%.

==========

**Isaac:** GNU Linux es muy importante en el ámbito de la seguridad. En nuestro blog hemos hablado de distribuciones como Santoku, Kali, BugTraq, Xiaopan, Parrot OS, WiFislax, DEFT, Backbox, IPCop, o de otras orientadas a la navegación segura y la privacidad, como Tails y Whonix. En vuestra rutina diaria ¿cuáles empleáis?

**Francisco Sanz:** Dependiendo del trabajo a realizar…por ejemplo, en pentesting yo uso una distribución propia (TPS) con herramientas de pentesting que usamos, pero con base en debían 7.

**Isaac:** Muchos atacan al software libre o de código abierto diciendo que es de mala calidad o que es más inseguro. ¿Qué le dirías a estas personas? ¿Consideras que es más fácil atacar a una máquina GNU Linux o FreeBSD por el hecho de ser de código abierto que una con Windows por ser código propietario o es al contrario?

**FS:** La pregunta del millón. O la pregunta de siempre. Para mí no es el sistema, sino la persona que configura el sistema.
Aun así, si tengo que decidir, siempre diría LINUX. Por qué? Hay muchas razones, pero por no extenderme te diría que su configuración por defecto es más segura que la de Windows; también puedes securizarlo más al tener múltiples opciones; al ser software libre, tú puedes desarrollar, modificar o ampliar servicios de seguridad.
Por otro lado, no hay ejecutables para que te puedan infectar con troyanos tan fácilmente. Aun así, parece que ahora es Windows el más seguro, según algunas publicaciones…o a lo mejor, el que más dinero tiene…no sé si me explico. En esa comparativa nombran 119 vulnerabilidades de linux Kernel..sin especificar…sin embargo aparecen 248 entre los sistemas Windows…pero especificando una cantidad inferior por cada S.O de Windows…es decir…un pequeño juego de números. Mucho marketing ;)

**Isaac:** The Security Sentinel es partner del proyecto Metasploit de Rapid7, un proyecto de código abierto, como tantos otros que se utilizan para el pentesting o el análisis forense. Es un buen ejemplo que deja patente lo que comentábamos en la anterior pregunta. ¿No crees?

**FS:** Bueno, Metasploit (Rapid7), lleva muchos años invirtiendo tiempo en desarrollos de exploits para vulnerar sistemas de todo tipo.
Creo que la posibilidad de que puedas desarrollar, modificar o ampliar los objetivos de un exploit y poder usarlo con una framework como este, sin tener que estar pagando o esperando a nuevos exploits, al ser de código abierto, te facilita muchísimo la labor.
Aunque existe una versión de pago, con la gratuita y con conocimientos de programación en ruby, Python, perl… tienes un compañero de trabajo muy, pero que muy útil.
También he de comentar, que muchos usuarios de Metasploit, sólo usan el 10 o el 20% de sus posibilidades. En el próximo curso de Hacking Ético que estamos desarrollando (CHEE), tenemos un tema entero para Metasploit, donde enseñaremos a utilizar la herramienta al máximo.

**Isaac:** Python es un lenguaje de programación bajo otra licencia libre (PSFL) y que tenéis muy presente en el sector de la seguridad. ¿Por qué? ¿Qué tiene de especial frente a otros?

**FS:** Python tiene una ventaja muy grande y son sus librerías. El uso de estas y la facilidad del aprendizaje del lenguaje, te ayuda mucho a poder realizar pequeñas tools que te son muy útiles a la hora de realizar una auditoría de seguridad basada en pentesting.
Además puedes conectar pequeños programas en Python con otros como nmap, nessus etc.. y esto te ayuda aun más a agilizar la labor de un pentester.
Nosotros sacamos un curso el dia 1 de Junio para nuestros alumnos, de Python para pentesters, porque creemos que es indispensable para un pentester utilizar este lenguaje.

**Isaac:** Últimamente se están detectando algunas vulnerabilidades críticas en proyectos de código abierto y algún que otro malware que ataca a sistemas GNU Linux. Las empresas que venden software cerrado, como por ejemplo Apple y Microsoft, tienen auditores de seguridad que atacan sus propios sistemas para mejorar la seguridad. ¿Crees que desde la comunidad de desarrollo de proyectos de código abierto se deberían plantear potenciar esta práctica?

**FS:** Bueno, crees que no existen auditores para Apache, Debian, Fedora, Ubuntu…otra cosa es que cobren lo que cobran los de otras firmas, pero existir, existen,pues entiendo que las grandes distribuciones tienen gente trabajando en esto. Sería ilógico no tenerlos. Además creo que todo esto

es una apuesta de futuro. El problema es, terminarán siendo las distribuciones más potentes de código abierto las nuevas Apple o Windows?

**Isaac:** Pasemos a los clientes de The Security Sentinel. Este verano estuve charlando con un ingeniero de Oracle y me comentaba que cada vez venden más servidores y supercomputadoras con Linux en detrimento de su propio sistema, Solaris, y que ellos incluso utilizan a diario para su trabajo una distribución denominada Oracle Linux. ¿Te encuentras cada vez más empresas que utilizan Linux o aun siguen dependiendo mucho de Windows?

**FS:** En este aspecto, te encuentras de todo.
Mis clientes ahora usan más Linux para servidores que Windows, pero los equipos de usuarios siguen siendo 90% Windows y un tanto por ciento muy elevado aun usan XP!!!

**Isaac:** Algunos gobiernos o empresas están migrando hacia distribuciones Linux por las posibilidades y ventajas que aporta. Algunos atraidos por la seguridad. ¿Animarías a las empresas y organizaciones a realizar este cambio? ¿TSS aconseja proyectos libres para alguna de las soluciones de seguridad que implantáis?

**FS:** Nosotros aconsejamos dependiendo de la necesidad de cada cliente. A mí me gustaría que la gente se volcase más con Linux, pero a veces el nombre de una marca pesa mucho.
Aun así, nosotros, siempre que podemos aconsejamos servidores Linux por su robustez, flexibilidad y seguridad.

**Isaac:** Muchos usuarios o empresas no prestan atención a la seguridad. ¿Hasta que punto es una mala práctica y qué consejos les darías? Cuéntanos algún caso grave que se pueda exponer y que hayas observado durante tu experiencia para concienciar al público.

**FS:** ¿Muchos? Casi nadie. Lo primero que les aconsejaría, sería que diesen un pequeño curso de concienciación sobre normativas básicas de seguridad informática.
Hasta en la Agencia Tributaria me he encontrado a usuarios con el post-it con su password en el monitor!
Pero increíble fue ver in situ, en una pequeña presentación de nuestra empresa en un posible cliente, que además es una empresa que juega con valores en bolsa (brokers), escuchar al director de operaciones desde su despacho, gritarle al informático “CUAL ES MI P…A CONTRASEÑA??!!” Aun después de ver esto, el posible cliente no nos contrató…que Dios les pille confesados!

**Isaac:** Ahora también impartís cursos sobre hacking y seguridad. Tú mismo realizastes el examen CEH (Council Ethical Hacking) de EC-Council y con una puntuación bastante buena. Existe un dicho que dice que “la mejor defensa es un buen ataque”, lo digo en referencia a la pregunta anterior. ¿Animarías a los usuarios a realizar este tipo de cursos?

**FS:** Yo les animaría a no centrarse en la «titulitis» y sí en realizar cursos para aprender. Nuestros cursos los centramos en la práctica, porque no me gustó este curso que tu nombras, ya que lo estudié por libre, y además sin prácticas. Solo es un título. Sin embargo, nuestros alumnos, se “machacan” haciendo prácticas. Sino que te lo digan a ti…
Un deportista debe entrenar todos los días. Nosotros también.

**Isaac:** Muchos creen que un hacker es una persona mala. Incluso la RAE lo define como un pirata informático que utiliza sus conocimientos para hacer cosas malas. Es triste escuchar esto, porque incluso ha obligado a que se tengan que ver términos como “ethical hacking” para que la gente no piense en un ciberdelincuente. Eric Reymond, defiende el término “hacker” con la definición

original y aboga por emplear “cracker” para referirse a los “malos”. Pero ante la maquinaria propagandística de Hollywood, que también se han encargado de crear mala reputación con multitud de películas y series sobre hackers, qué se puede hacer… ¿Qué opinas como experto en seguridad?

**FS:** Yo considero la palabra hacker como un especialista en informática que investiga de forma a veces obsesiva hasta encontrar su respuesta. Pero de ahí a la delincuencia… Por supuesto que hay hackers que son delincuentes, como puede haber bomberos que también lo sean. Pero al igual que no se generaliza en el segundo caso, por qué hacerlo en el primero? En definitiva, creo que la RAE muestra una gran incultura a la hora de denominar la palabra hacker como pirata informático. Lo de Hollywood es mejor ni mentarlo…