Arturo Ribagorda

DETECCIÓN DE INTRUSOS
Guía avanzada - 2ª edición

Autores: Stephen Northcutt, Judy Novak
Editorial: Prentice Hall/Pearson Education
Año 2001 - 445 páginas - ISBN: 84-205-3115-4
Sitio: www.pearsoned.es / www.diazdesantos.es

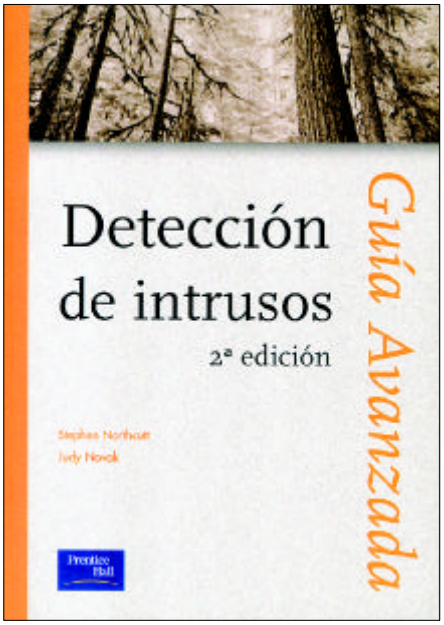
Las primeras medidas que se consideran cuando se desea proteger cualquier bien frente a alguna amenaza son las de prevención, que tratan de evitar la materialización de dicha amenaza –es decir, el ataque– o, si ello no es posible, que el mismo ni siquiera penetre el sistema de defensa. Sin embargo, también es sabido que, siendo cualquier medida de seguridad vulnerable, no es prudente confiar toda la protección a un único tipo de medidas. Por ello, se instrumentan –comúnmente en segundo lugar– otros tipos adicionales de medidas, entre las que sobresalen las de detección.

Naturalmente, todo lo dicho es también aplicable a la seguridad de los sistemas de información, hoy en día conformados en redes de ordenadores. Prueba de ello la tenemos en la atención que en los últimos años suscita la detección de intrusiones, basada ordinariamente en sistemas así denominados, y usualmente abreviados por sus siglas en inglés, IDS (*Intrusion Detection System*).

Y es que, en efecto, si durante la época de rauda expansión de las redes de ordenadores –los años iniciales de la pasada década de los noventa– el interés de los profesionales de la seguridad se ceñía a los cortafuegos –sistemas de prevención–, en el presente, y ya desde hace algunos años, su punto de mira se ha desplazado –sin que ello suponga una minusvaloración de los cortafuegos– a los sistemas que motivan el libro que reseñamos, en otras palabras, a las medidas de detección.

Lógicamente, ello no podía dejar de notarse en la bibliografía, que así está viendo aparecer numerosos manuales centrados en estos sistemas, uno de los cuales es el que nos ocupa en esta ocasión. El libro, de título en castellano: **Detección de Intrusos**, es traducción de la segunda edición (aparecida en el año 2001) de *Network Intrusion Detection. An Analyst´s Handbook*., escrito por dos profesionales de amplia experiencia en la protección de redes: Stephen Northcutt y Judy Novak, y publicado por la editorial Prentice Hall.

Redactado desde la amplia experiencia acumulada por sus escritores, en el volumen encontrará el lector una abundantísima colección de ejemplos y situaciones reales, así como detallados consejos de cómo interpretar los registros obtenidos mediante variadas herramientas de análisis (cuyo funcionamiento también se pormenoriza), casi siempre desarrolladas para el mundo Unix, aunque ocasionalmente también para plataformas NT. Igualmente, se hallarán numerosas y diversas medidas de seguridad –no sólo, aunque principalmente, de detección, sino también de prevención–, y técnicas de gestión y respuesta ante incidentes.



Pero, esbozado el contenido y entrando ya en la crítica, lo primero que sobresale en la obra es el público (lector) objetivo, constituido evidentemente por profesionales de la seguridad que desarrollan su quehacer en la protección de redes. Ello se pone de manifiesto en la muy reseñable exhaustividad –tanto en amplitud como en profundidad– con que se contempla la materia, que será de utilidad y hará las delicias de los dedicados a la seguridad de la redes, y a buen seguro les ilustrará en situaciones a las que se enfrentan cotidianamente. Naturalmente, esta misma minuciosidad en el tratamiento, hará la lectura de muchas de sus partes tediosa a aquellos otros expertos más generalistas o especializados en otros campos, de los muchos, que conforman en el presente la seguridad.

La segunda nota a destacar, positivamente, es la actualidad de los ataques que describe, las herramientas de detección que presenta y los procedimientos de análisis y obtención de evidencias que detalla. Y es que, si bien a cualquier libro escrito en un cierto año (en el que nos ocupa, el 2001 en su versión original) se le debe suponer –siquiera meses más tarde– dicha puesta al día, ello no siempre ocurre, y a menudo nos hemos encontrado, en estas mismas recensiones, publicaciones ya obsoletas el mismo día de su aparición en las librerías.

Finalmente, y aún en el haber, cabe ponderar la ajustada extensión y claridad expositiva con que se presentan los protocolos básicos de Internet en los capítulos primero y segundo. Y lo mismo cabe decir de los primeros apartados de los capítulos tercero, cuarto y sexto (de nombres respectivos: Fragmentación, ICMP y DNS), en los que se tratan los protocolos y servicios de dicha red, que son en ocasiones el objeto y otras veces el medio de los ataques a la red de redes.

Sin embargo, y ya en el debe, es manifiesta la falta de estructuración de la obra, cuya exposición hubiese resultado más sistemática y didáctica de haberse articulado en dos o tres grandes bloques temáticos, en los que se hubiesen podido enmarcar los capítulos que la componen. De otro modo, como ha ocurrido, queda una mera yuxtaposición de los mismos (de hasta 22, que no menos la componen) sin engarce ninguno entre ellos. Y aún más, con algunos aspectos (como los ataques smurf, Trinoo, TFN, etc) estudiados en diversas partes. De esta forma, la obra peca de una vasta acumulación de conocimientos –bastante parecida a un totum revolutum–, muy interesante sin duda para el público al que va destinada, pero difícil de asimilar aun para éste.

Por otro lado, y en este mismo orden de aspectos mejorables, se debe citar la labor de los traductores, cuestión ésta reiteradamente señalada en estas mismas líneas en las obras dobladas a nuestra lengua. Y es que la amplitud alcanzada, en el momento actual, por la disciplina de la seguridad hace que sean muchos los matices singulares de los términos usados en la misma, lo que precisa de traductores no ya expertos en informática sino en seguridad. Esta carencia de conocimientos específicos en la disciplina queda notoriamente patente desde el mismo prefacio del volumen.

En síntesis, es una obra muy notable (se diría que imprescindible) para los analistas de seguridad en redes que, sin embargo, hubiese resultado mucho más provechosa para los mismos de haber estado mejor estructurada. De esa manera, además, hubiese sido de lectura recomendada no sólo para dichos profesionales, sino también para cualquier otro de la seguridad, independientemente de su campo de trabajo. n

Arturo Ribagorda
Catedrático de la Universidad
Carlos III de Madrid