Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Comparativa de herramientas de seguridad (16708 lectures)

Per **Ricardo Galli Granada**, ***gallir*** (http://mnm.uib.es/gallir/)

Creado el 05/01/2001 00:00 modificado el 05/01/2001 00:00

> *Network Computing ha hecho una comparativa de los 8 detectores de vulnerabilidades mas conocidos. Ninguno fue capaz de detectar todas (17), pero Nessus gana (15).*

Es muy curioso el test[1] de Network Computing[2], se probaron los siguientes: Axent Technologies' NetRecon, BindView Corp.'s HackerShield, eEye Digital Security's Retina, Internet Security Systems' Internet Scanner, Network Associates' CyberCop Scanner, and two open-source products: Nessus Security Scanner and Security Administrator's Research Assistant (SARA).

Para los test se usaron 17 vulnerabilidades bien conocidas en varias plataformas[3]: HP-UX 10.20, Linux RH6.2, MS NT 4, Netware 5.1 y Solaris 2.6. Las vulnerabilidades que tenían que detectar eran muy conocidas en sus respectivas plataformas, tales como wu.ftpd buffer overflow, sendmail buffer overflow, export del root en NFS, guest account, NULL sessions, RDS, script Cold Fussion, etc (mas detalles en un PDF[4]).

Ninguno pudo detectar los 17 fallos, aunque el ganador fue Nessus[5], con 15 vulnerabilidades detectadas. Las posiciones finales fueron:

1. **Nessus: 15** (*OpenSource*)
2. Internet Security Systems Internet Scanner: 13.5
3. Axent technologies NetRecon 3.0: 13
4. BindView HackerShield: 12
5. NA CyberCop Scanner: 12
6. **SARA: 10** (*OpenSource*)
7. **World Wide Digital Security SAINT: 9** (*OpenSource*)
8. eEye Digital Security Retina: 6.5

Está muy bien que un programa *OpenSource* sea el ganador, pero lo más curioso es que el Nessus no pudo detectar el *Sendmail buffer overflow* ni el *wu-ftpd buffer overflow*, ambas muy conocidas y las primeras en ser probadas por cualquier "crackersillo".

También llama la atención que SARA ni SAINT hayan sido capaces de detectar el directorio FTP /pub sin protección de escritura. También esta claro en el test que SAINT es muy malo para detectar fallos graves en el Solaris 2.6.

Para los interesados en herramientas de seguridad, ésta de insecure.org[6] es una lista muy completa.

Lista de enlaces de este artículo:

1. http://www.nwc.com/1201/1201f1b1.html
2. http://www.nwc.com/
3. http://www.nwc.com/1201/1201f1b5.html
4. http://img.cmpnet.com/nc/1201/graphics/f1-detect-results.pdf
5. http://www.nessus.org/
6. http://www.insecure.org/tools.html

E-mail del autor: gallir _ARROBA_ uib.es

Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=378