

BIBLIOGRAFÍA

Detección de intrusos en la red: más allá del NIDS

David Pérez, Consultor independiente

En la Web

- *RaDaJo (Blog del ponente, David Pérez, junto con Raúl Siles y Jorge Ortiz)*
<http://www.radajo.com>
- *The SANS Institute*
<http://www.sans.org>
- *RFC 1510: The Kerberos Network Authentication Service (V5)*
<http://www.ietf.org/rfc/rfc1510.txt>
- *Interpreting the NT Security Log - Use the Security Log to track user's activities*
<http://www.microsoft.com/technet/archive/winntas/support/usesecur.mspx?mfr=true>
- *Audit Account Logon Events*
<https://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/monitor/logvnts.msp>
- *Interpreting the NT Security Log - Use the Security Log to track user's activities*
<http://www.microsoft.com/technet/archive/winntas/support/usesecur.mspx?mfr=true>
- *Windows 2000 Kerberos Authentication*
<http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/kerberos.msp>
- *Microsoft Script Center*
<http://www.microsoft.com/technet/scriptcenter/default.msp>

Herramientas

- *Scripts útiles para administración de sistemas Windows*
<http://www.isascripts.org>
- *Snort*
<http://www.snort.org>
- *WireShark*
<http://www.wireshark.org>

Productos Niksun (network forensics)

- <http://www.niksun.com>

PowerShell

- <http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx>