Honeynet Project's FC2010/2 - My submission

publié par malphx le mercredi, mars 24 2010 - 13:48



The second 2010´char(180) Forensic Challenge published by the Honeynet Project is now closed, and the results have been published.
This time the investigators (or contestants) had to dissect a pcap file containing network traces of browsers under attack.
The analysis revealed that a lab setup has been used to mimic the interactions between victim's browsers and some malicious Web sites.
Feel free to review my submission, all the winners submissions and the solution given by the Honeynet Project's Team.
I haved scored 43/43 for this one, and so I'm one of the 4 winners
I'm now waiting the publication of #3 ('Banking Troubles'), which promises to be very interresting.
Finally, I would also like to thank all the Honeynet Project's team for giving us such interresting and educationnal contests !