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 !

Honeynet: Challenge 1 of the Forensic Challenge 2010

publié par malphx le mardi, février 16 2010 - 13:49

I've participated in the last Honeynet Challenge.
This Challenge ran from Jan 18th 2010 to Feb 15th 2010.

It was about the analysis of a PCAP trace file containing an attack.
Results have been published,
 and I'm proud of my #2 position in this contest.
You could find my submission on The Honeynet Project's website.