Honeynet data capture - practical analysis session 1

Alexandre Dulaunoy

ASBL CSRRT-LU (Computer Security Research and Response Team Luxembourg)
http://www.csrrt.org/

30th November 2005

Session
Part 1
Part 2
Part 3
Part 4/work
Q and A

Part 1

Make a simple script (one-liner accepted) using the tools we saw in the workshop to extract all of the payloads from the capture and classify the data by type ?
hints : tcpflow, magic number, ...

Session
Part 1
Part 2
Part 3
Part 4/work
Q and A

Part 2

Based on the files collected ? can you assume specific events ?

hints : filename, content, ...

Part 3

If you were an attacker and you have compromised a system. How do you hide yourself ? (assuming a GNU/Linux system connected to Internet with a simple web server)

Part 4/work

Extract all IPs, give information about the unique source (e.g. localization) and tcp services/per country/sources. Graphics are welcomed.

Q and A

- Thanks for listening.
- http://www.csrrt.org.lu/
- adulau@foo.be