CSIRT exercises

27th TF-CSIRT
18th / 19th May 2009,
León, Spain

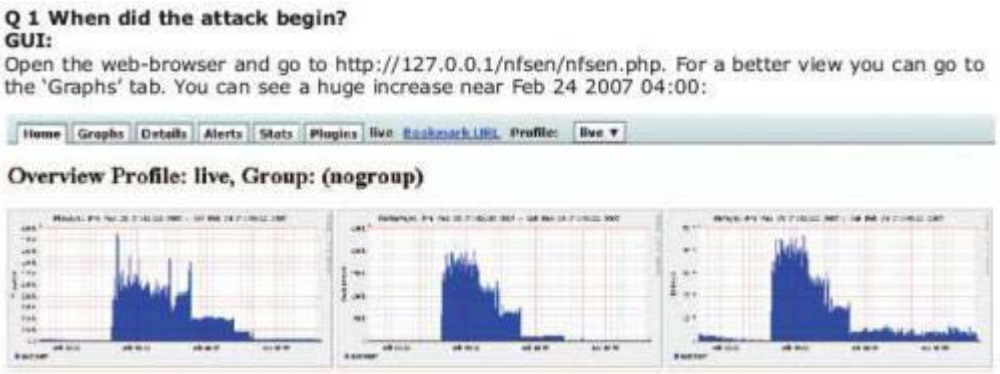
Marco Thorbruegge, ENISA
Przemek Jaroszewski, CERT POLSKA

Main deliverable 2008: CSIRT Exercise material

A students version …

… a teachers version …

… plus Live-DVDs …



… EXERCISE! Based on "real" life examples!

Main deliverable 2008: CSIRT Exercise material

CERT Exercises Handbook

Table of contents

Activities in 2009
CSIRT Exercise Pilot

Exercise 9
Large-scale Incident Handling

WHAT WILL YOU LEARN?

The purpose of this exercise is to introduce you to the way large-scale incidents can be handled. You will face different scenarios, presented by the trainer. For each scenario, follow carefully what the trainer has to say. The trainer will explain a certain initial situation and you will be asked to suggest ways of moving forward. To help you, the trainer will pose leading questions. Answering the questions will move you to the next phase of the scenario, until you arrive at the final solution.

EXERCISE TASKS

PART 1 LARGE-SCALE PHISHING ATTACK
This exercise is meant to be carried out with the help of the trainer. At the beginning, you will be given a short overview of what phishing is. The trainer will then present a scenario to you. The scenario will be resolved through a series of steps (tasks).

Task 1	Source of information
	What are your possible sources for obtaining information about phishing incidents?

Task 2	Initial investigation
	What would be your first steps in tackling a reported phishing incident?

+

The material ... ... plus ... ... real CERTs ...

=

- Case study
- Usability assessment
- New ideas

... equals ... ... **Improvement!**

Outlook: plan for 2010

WPK 2.2

- Good practice in providing CERT services
  - based on the survey from 2009
- Facilitate cooperation and information sharing
  - pan-European cooperation among national / governmental CSIRTs
- 5th ENISA Workshop (CERTs in Europe)
  - the role of national / governmental CSIRTs in national and international exercises
- Continue facilitation of the setting up of CERTs
  - continue to develop tools for strengthening the CERT community

Featuring ....

Real life incident handling case studies

Od: UKSUtopia Inspections <control@ministry.gov.ut>
Data: 2007-11-05 07:54
Do: SPAM <spam@cert.ut>

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

John.S@ministry.gov.ut
(generated from John.Smith@ministry.gov.ut)
mailbox is full: retry timeout exceeded

------ This is a copy of the message, including all the headers. ------

Return-path: <control@ministry.gov.ut>
Received: from [10.7.56.1201 (helo=K1292K3027)

Mail delivery f...e to sender.eml

Keys to the exercise

Task 1 UKSUtopia Inspections

This may seem like a regular spam report. On closer analysis it turns out that apparently somebody at *control@ministry.gov.ut* sent a message to a mailing list informing co-workers about some scheduled maintenance. One of the addresses bounced and the bounce message was reported as spam. Clearly, this is a misunderstanding and the report is void.

Management skills exercises

Appendix A

Job Advertisement for IT Security Specialist (Incident Handling Service)

Main tasks:

- Handling network security incidents
- Operating the CERT early warning and alerting system for a CERT constituency
- Writing security advisories
- Writing security news
- Preparing CERT reports

Essential requirements (technical qualifications, knowledge and personal skills)

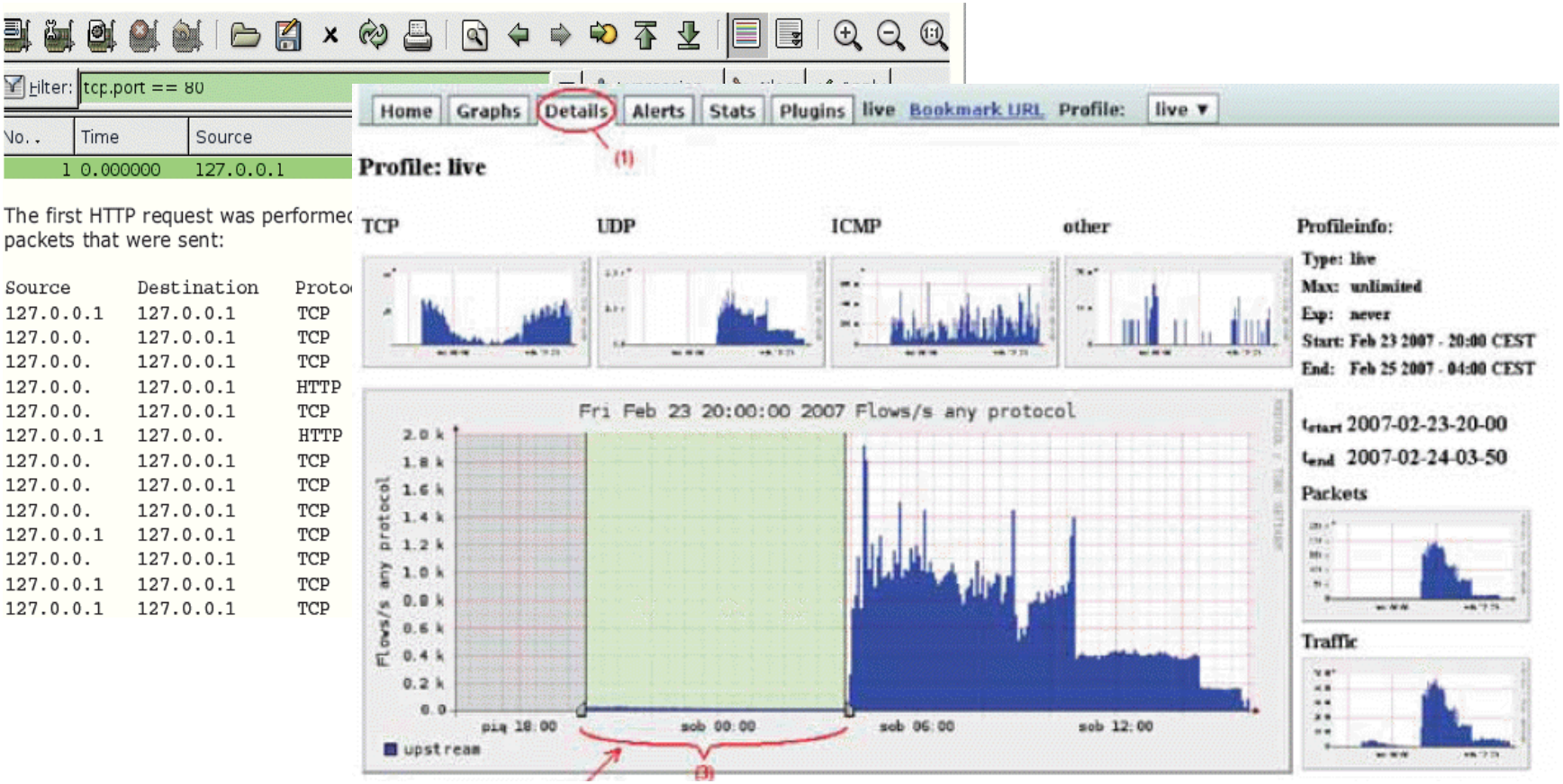
- .....
- .....
- .....

Role playing games

ERNEST – You are an employee of Ads-R-Us, a leading marketing company in the country, servicing large and well-known businesses. Actually, you are one of the network administrators to whom the role of a CSIRT officer in the company has been delegated as part of your duties. You keep in touch with your ISP and the vendors of your most critical business applications, ie, Munix, the providers of a great OS that facilitates group work and VPN software to access it, and Office Painters, the authors of the designer's software suite.

WINSTON – You are the CEO of Ads-R-Us, a leading marketing company in the country, servicing large and well-known businesses. Since you are quite busy with your own job, you tend to rely on trusted employees to get most of the work done rather then getting yourself too involved. You also value spending days off with your family without being too distracted. And there you go, it is just another Saturday morning, a perfect time to sit back in the garden with your daughter's birthday party scheduled for the evening.

Technical stuff



… and much more!

Pilot exercise sessions planned

- 3rd June 2009 – Chisinau, MD
  - Large Scale Incident Handling (and more)
  - Collocated with CLOSER coordination meeting - mostly CERTs from former USSR
- 30th June 2009 – Kyoto, JP
  - Network Forensics
  - During FIRST conference – FIRST members

Questions?

Contact:

Marco Thorbruegge
Senior Expert Computer Security and Incident Response
Cooperation and Support Department
+30.2810.39.1372
cert-relations@enisa.europa.eu