|  |
| --- |
| OTO Oefening – KPN-CERT |
|  |
| Technical exercise for KPN-CERT and other interested parties |
|  |
| For internal use |
|  |

# Exercise Goals

This exercise concerns a digital forensic investigation, as carried out by KPN Security/KPN-CERT, based on a network forensic capture in PCAP format. It is a copy of the LMG Network Forensics Puzzle contest training (<http://forensicscontest.com/2009/09/25/puzzle-1-anns-bad-aim>). The challenge combines the knowledge and skills that are (among other) part of the GIAC Network Forensic Analyst certification. Tools / solutions to these challenges are often integrated into the SANS GIAC Network Forensics Analyst coursework and toolkits.

The ‘win condition’ of this exercise is a comprehensive set of answers to the questions, through analysis of the historical events in the Packet Capture.

# Requirements

* A work room
* PCAP file <http://forensicscontest.com/contest01/evidence01.pcap> + MD5
* Time: 1-2 hours – max. 15 minutes explanation and evaluation
* Attendees:
  + Laptop suitable for digital forensic investigation of network-captures with Wireshark, e.g.: DEFT, SIFT, Kali

## Structure

* One MC: KPN-CERT, covering both guiding of content and process
* Attendees fulfil their usual role (SOC, Security or CERT)

## Rules

* Cooperation should be limited, in order to prevent:
  + Answers from being shared
  + Few people actually working on the exercise

# Description

Anarchy-R-Us, Inc. suspects that one of their employees, Ann Dercover, is really a secret agent working for their competitor. Ann has access to the company’s prize asset, the secret recipe. Security staff are worried that Ann may try to leak the company’s secret recipe.

Security staff have been monitoring Ann’s activity for some time, but haven’t found anything suspicious– until now. Today an unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann’s computer, (192.168.1.158) sent IMs over the wireless network to this computer. The rogue laptop disappeared shortly thereafter.

“We have a packet capture of the activity,” said security staff, “but we can’t figure out what’s going on. Can you help?”

**3.1 Questions**

**3.1.1 What is the name of Ann’s IM buddy?  
  
‘**sec558user1’ - this can be comparatively easily determined from examining the PCAP file. Ignoring or filtering out the through the non-relevant traffic, such NetBIOS etc., shows packets being ‘dissected’ as SSL by Wireshark, but actually contain plaintext. Ann’s computer initiaties an AIM conversation with the ‘sec558user1’ handle.

**3.1.2 What was the first comment in the captured IM conversation?  
  
“***Here’s the secret recipe… I just downloaded it from the file server. Just copy to a thumb drive and you’re good to go >:-)”.* The method for this is identical to question 3.1.1.

**3.1.3 What is the name of the file Ann transferred?***recipe.docx.* After the exchange of messages, Ann initiates an OFT2 file transfer with the sec558user1, where the filename is visible. This can also be seen when examining the TCP stream, by right-clicking in Wireshark’s top window and selecting Follow → TCP-stream.

**3.1.4 What is the magic number of the file you want to extract (first four bytes)?**0x504B0304 (Note: one byte = 8 bits = 2 hex digits!). Extracting the *recipe.docx* file can be done in multiple ways:

1) Follow TCP stream and then either

2a) Selecting only Ann’s TCP traffic and saving the file to disk as RAW data (from the TCP stream), stripping off the first 256 bytes with dd (dd if=input of=output bs=1 skip=256)  
2b) Copying and pasting the RAW hex data, opening a terminal window, type ‘*cat -|xxd -r -p > recipe.docx’* and pasting the contents of the clipboard into that terminal window.

***3.1.5* What was the MD5sum of the file?**8350582774E1d4dbe1d61d64c89e0ea1 recipe.docx (md5sum …)

**3.1.6 What is the secret recipe?**

The resulting file should be recognized as Microsoft Word 2007+ by the file command.  
 ***“****Recipe for Disaster:  
1 serving  
Ingredients:  
4 cups sugar  
2 cups water  
In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.”*

**4 General guidelines**

The PCAP should be loaded into Wireshark.

Easiest solution methods probably involve:

* Filtering for the IP addresses found
* Evaluating data fields/payloads manually, since the PCAP filesize is limited
* Extracting all objects and analyzing them