

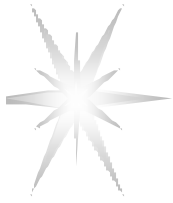
Clearinghouse for Incident Handling Tools

4th TF-CSIRT Meeting

September 28, 2001

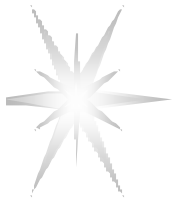
Manchester

Yuri Demchenko <demchenko@terena.nl>



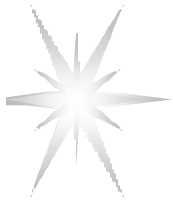
Agenda

- Clearinghouse goals
- Questionnaire
 - ◆ Structure of the Questionnaire
 - ◆ Preliminary classification of tools
 - ◆ Privacy issues
 - ◆ Summary of responses
- Summary
- Clearinghouse structure
- Follow on activity



Clearinghouse goals

- Creating repository of popular tools
 - ◆ Creating collection of recommended/common tools
 - ◆ Ranking and evaluating tools
- Experience exchange
 - ◆ Collections of Procedures and Practices used by CSIRTs to collect Incident Data/Evidence, Investigate and Track Incidents
- Easy setting up work procedure for new CSIRT teams
- Provide collective feedback for manufactures and developers



QUESTIONNAIRE about Tools, Procedures and Practices

The Questionnaire attempts to cover wide range of information which we would like to collect from and exchange between CSIRTs

Questionnaire contains two parts:

- Part 1. Sections A, B.
GENERAL Questions where you are questioned about future Clearinghouse structure,
- Part 2. DETAILS on used tools - Sections 1-6.

Text version of the Questionnaire

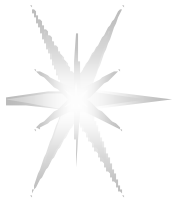
<http://www.terena.nl/task-forces/tf-csirt/tf-csirt-chiht-q.txt>

RTF version of the Questionnaire

<http://www.terena.nl/task-forces/tf-csirt/tf-csirt-chiht-q.rtf>

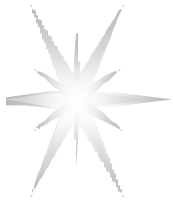
Proposed format of Summary

<http://www.terena.nl/task-forces/tf-csirt/tf-csirt-chiht-01.html>



Preliminary classification - Categories of Tools

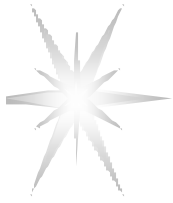
1. Incident Data/Evidence Collection
 - 1.1. Tools for examining Hard Disk
 - 1.2. Utilities for examining systems and processes
2. Investigative tools
 - 2.1. Extracting information from collected data/Evidence
 - 2.2. Checking Attacker and Victim Identity (including network contact information)
3. Tools to support CSIRT procedures
4. Tools for recovering compromised system
5. Pro-active tools
6. Secure Remote Access Tools



Information about tools

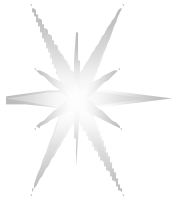
- Tool/program name
- OS and/or file system
- Short description, definition, URL to download, manual
- Run on dedicated machine or user machine
- Use of tool on working system or detached from network
- Use on Evidence machine/disk or on image disk/system

Different information applicable to different categories of tools



Questionnaire - Privacy issues

- Questionnaire is for INTERNAL PURPOSES of TF-CSIRT
- Any public use of gathered data will be based on formal consent of responding CSIRT
- All private information about particular CSIRT will be removed from the Summary and publicly available documents



Questionnaire - Summary

5 responses received so far

- BTCERTCC
- BT Ignite Solutions
- UNIRAS
- CERT-DK
- IRIS-CERT
- CERT-NL
- JANET-CERT
- CERT-NL
- SUNET-CERT
- FUNet CERT
- GARR-CERT



Summary: Specific groups of tools used by CSIRTs

[*] [*] [*] [*] [*] [*] [] [] [] [] Data/Evidence collection (Forensics)

[*] [*] [*] [*] [*] [*] [] [] [] [] Incident Investigation

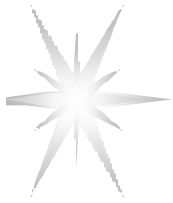
[*] [*] [] [] [] [] [] [] [] [] Data/System recovery

[*] [*] [*] [*] [*] [*] [*] [*] [] [] Incident tracking and reporting

[*] [*] [*] [*] [*] [*] [*] [*] [] [] Pro-active tools

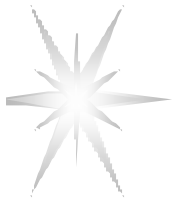
[*] [] [] [] [] [] [] [] [] [] Secure remote access

[*] [] [] [] [] [] [] [] [] [] Other: links to tools



Summary: Clearinghouse Components

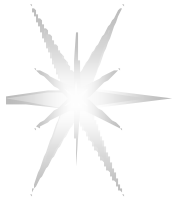
- [*] [*] [*] [*] [*] [*] [*] [*] [*] [*] [*] List of tools (forensic, investigative, proactive, data recovery, tracking, etc.)
- [*] [*] [*] [*] [*] [] [] [] [] [] [] Repository/Archive of popular tools
- [*] [*] [*] [*] [*] [*] [*] [*] [*] [] [] Description/use of tools
- [*] [*] [*] [*] [*] [*] [] [] [] [] [] Collection/Repository of Incident Handling procedures (forensic, recovery, investigative)
- [*] [*] [*] [+] [] [] [] [] [] [] [] Formal requirements for different groups of Incident Handling tools (and procedures)
- [*] [] [] [] [] [] [] [] [] [] [] Other: (1) links to similar websites



Questionnaire – follow-on activity

Some kind of consulting efforts (possibly in a form of Pilot Project) needed to do such works as

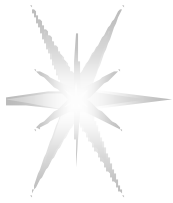
1. Requirements to Incident Handling (including Forensics) tools
2. Forensic CD with collection of tools
3. Compilation of Incident handling procedures



Clearinghouse – Next steps

Clearinghouse of Incident Handling Tools

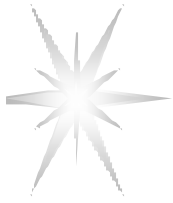
- **Publish Summary of the Questionnaire on tools and practices used by CSIRT Teams**
- Create repository of tools in different categories
 - ◆ Manuals/Tutorials are very desirable
- Prepare list of recommended tools for different CSIRTs procedures (investigation, incident tracking, etc.)
- Include basic/recommended tools into Training Programme/materials
- **Consider moving permanent Clearinghouse to one of CSIRTs**



Requirements (1): Data/Evidence collection tools

Actions required during Incident data (Evidence) collection

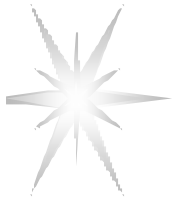
- processes examining
- examining system state
- examining physical and logical HD
- programs for generating core images and examining them
- Document/e-mail retrieval/search
- Programs/scripts to automate evidence collection



Requirements (2): Investigative tools

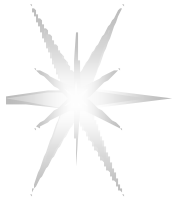
Actions required during Incident data analysis/investigation

- Checking Attacker and Victim identity
 - ◆ IP -> DN, DN -> IP
 - ◆ Contact, network data
- Extracting information from collected data and CSIRT archives
 - ◆ Extended log file analysis
 - Based on library of rules
 - ◆ Tracking similar cases



Requirements (3): Tools to support CSIRT procedures

- Support CSIRT procedure
 - ◆ Incident registration
 - ◆ Incident tracking
 - ◆ Incident reporting
- Easy configurable
 - ◆ Web-based interface
- Customer support (call center) – optional?



Requirements (4): Pro-active tools

- Network Auditing (Security Scanners)
- Host-based Auditing
- Security Management
- Network monitoring and traffic analysing
- Network IDS