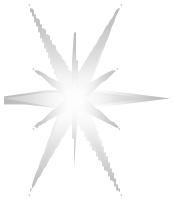
Clearinghouse for Incident Handling Tools

3rd TF-CSIRT Meeting

June 1, 2001

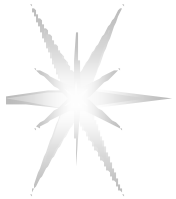
Ljubljana

Yuri Demchenko <demchenko@terena.nl>



Agenda

- Clearinghouse goals
- Questionnaire
  - Structure of the Questionnaire
  - Preliminary classification of tools
  - Privacy issues
  - Summary of responses
- 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.

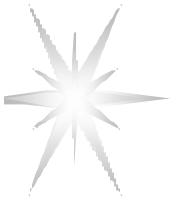
Text version of the Questionnaire
http://www.terena.nl/task-forces/tf-csirt/tf-csirt-chiht-q.txt

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

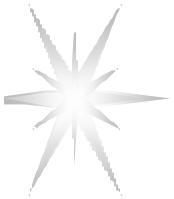
1. Incident Data/Evidence Collection
   1.1. Tools for examining Hard Disk
   1.2. Utilities for examining systems and processes
2. Investigative tools
   2.1. Extracting information from collected data/Evidence
   2.2. Checking Attacker and Victim Identity (including network contact information)
3.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



Information about tools

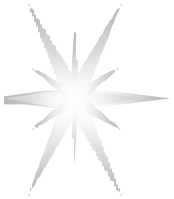
- Tool/program name
- OS and/or file system
- Short description, definition, URL to download, manual
- Run on dedicated machine or user machine
- Use of tool on working system or detached from network
- Use on Evidence machine/disk or on image disk/system

Different information applicable to different categories of tools



Questionnaire - Privacy issues

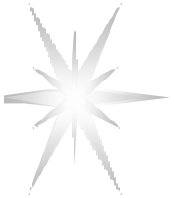
- Questionnaire is for INTERNAL PURPOSES of TF-CSIRT
- Any public use of gathered data will be based on formal consent of responding CSIRT
- All private information about particular CSIRT will be removed from the Summary and publicly available documents



Questionnaire - Summary

5 responses received so far

- BTCERTCC
- BT Ignite Solutions
- UNIRAS
- CERT-DK
- IRIS-CERT



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

Summary: Clearinghouse Components

[*] [*] [*] [*] [*] List of tools (forensic, investigative, proactive, data recovery, tracking, etc.)

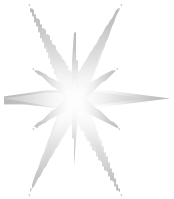
[*] [*] [*] [*] [ ] Repository/Archive of popular tools

[*] [*] [*] [*] [*] Description/use of tools

[*] [ ] [*] [*] [*] Collection/Repository of Incident Handling procedures (forensic, recovery, investigative, etc.)

[*] [ ] [+] [*] [ ] 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

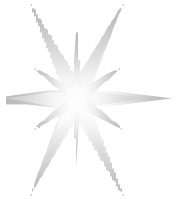
Clearinghouse of Incident Handling Tools

- **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**

FAQ: How to submit you response to the Q.?

1) Read Questionnaire
2) Check example of the Summary whether you understand all questions correctly
3) Fill in Questionnaire
4) Send to demch@terena.nl



Requirements (1): Data/Evidence collection tools

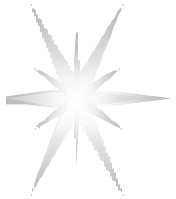
Actions required during Incident data (Evidence) collection

- 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

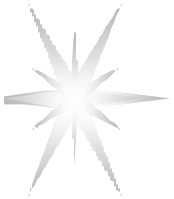
Actions required during Incident data analysis/investigation

- 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



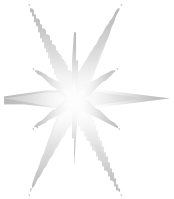
Requirements (3): Tools to support CSIRT procedures

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

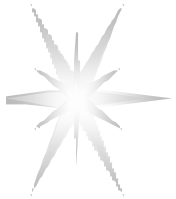


Requirements (4): Pro-active tools

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



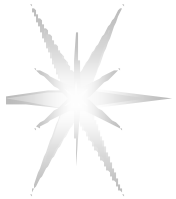
Clearinghouse: Recommended groups of tools



Recommended Evidence collection tools set

http://www.ietf.org/internet-drafts/draft-ietf-grip-prot-evidence-01.txt

- Forensics CD should include the following
  - a program for examining processes (e.g., 'ps').
  - programs for examining system state (e.g., 'showrev', 'ifconfig', 'netstat', 'arp').
  - a program for doing bit-to-bit copies (e.g., 'dd').
  - programs for generating core images and for examining them (e.g, 'gcore', 'gdb').
  - scripts to automate evidence collection (e.g., The Coroner's Toolkit)
- The programs on the forensics CD should be statically linked, and should not require the use of any libraries other than those on the CD.



Investigative tools – CERT UKERNA Example

about - obtains information from DNS and whois servers for a given IP address or name; checks the current CERT mailboxes and router logs to see if the IP address has been reported in other contexts

apnic, arin, ripe - look up details of a numeric IP address in the APNIC, ARIN or RIPE

gross - script to distill information from some supplied router log files. Attempts to identify hosts probed, start and end times of probing and ports probed.

eh - script to identify well-known portnumbers

findref - script to search for a string in JANET-CERT mailboxes (open, closed or all)

keykatch - script to extract contact information only from RIPE, ARIN and APNIC db

soa - script to find the e-mail address responsible for the DNS server in a domain e.g.

internic - script to query the InterNIC for details about some networks

ip2host - public domain script to take a file of IP addr. and convert them to hostnames

janic - script to query the JANET whois server for details about .ac.uk domains

nameof - script to translate a numeric IP address into a name

Incident tracking tools – Examples

- Action Request System from Remedy (ARS)
  - Web-based user self-support
  - Easy configurable
  - Integration with Network Management packages
- Magic Total Service Desk (Magic TDS)
  - Web-based customised interface
  - Network Oriented and scalable up to 1000 nodes
  - SNMP support (traps, etc.)
  - XML built and database format customisation
  - Based on MS DNA: Support VB abd COM scripts
  - Enables end-users to send requests via e-mail
- Nortel's Clarify