Clearinghouse for Incident Handling Tools

TF-CSIRT Seminar
January 18, 2001
Barcelona
Agenda

• Clearinghouse goals
• Tools used by CSIRTs
  ◆ Evidence Collection tools
  ◆ Investigative tools
  ◆ Incident tracking/reporting tools

• Remedy Action Request System by Andrew Cormack, CERT UKERNA

• Recommendations
  ◆ How to proceed?
Clearinghouse goals

- Experience exchange
  - E.g., library of rules for Intrusion/Activity detection
  - Can we do it in effective way?
- Easy setting up work procedure for new CSIRT teams
- Simplify information exchange
- Provide collective feedback for manufactures and developers
- Possible establishing recommended/common tools set
Tools used by CSIRTs

- Evidence collection tools
- Investigative tools
- Proactive tools
- Incident registration and tracking tools
  - Support CSIRT procedure
  - Customer support (call center)
Evidence collection tools – Requirements 1

Actions required during Incident data (Evidence) collection

- processes examining
- examining system state
- program for doing bit-to-bit copies
- programs for generating core images and for examining them
- Programs/scripts to automate evidence collection
Recommended Evidence collection tools set


- 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 – Requirements 2

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
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 – Requirements 4

• Support CSIRT procedure
  ◆ Incident registration
  ◆ Incident tracking
  ◆ Incident reporting

• Easy configurable
  ◆ Web-based interface

• Customer support (call center) – optional?
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

• Clarify
Recommendations or How to proceed?

Clearinghouse of Incident Handling Tools

• Create repository of investigative tools for incident/evidence collection
  ◆ Manual/Tutorial is very desirable
• Prepare list of recommended tools for Incident tracking
• **Questionnaire on used tools and practices to CSIRT Teams**
• Include basic/recommended tools into Training Programme/materials
• Develop common tools and/or recommendations to make Incident/CSIRT information exchangeable
  ◆ Think about IODEF implementation