Practical Experiences with the deployment of honeypots

NoAH Workshop / TNC Catania
17 May 2006

DFN-CERT Services GmbH
Jan Kohlrausch / CSIRT

Introduction

- DFN-CERT: Computer Emergency Response Team for German research network (DFN).
- World-wide community of CERTs / CSIRTs.
- Constituency are mainly German universities and research institutes.

Introduction

- Basic services of a typical CSIRT
  - Incident Response and Incident Coordination
    - Analysis of incident.
      - How was the host compromised?
      - Which sites are affected?
      - Did the attacker leave behind any malicious software (*malware*) or exploits on the compromised host?
    - Sending incident reports including compromised hosts to all affected sites (incident Coordination).
    - Providing support to constituent sites to resolve from the incident (Incident Response).

Introduction

- Basic services of a typical CSIRT
  - Advisory service
    - Centralized announcement of vendor advisories (e.g. Microsoft security advisories).
    - Usually, updates or patches are provided.
  - Alerting service
    - Publication of alerts concerning
      - Zero-day exploits
      - Detection of new vulnerabilities (e.g. in common server programs or web-brosers).
      - Widespread exploitation of known vulnerabilities.

Introduction

- Honeypots at the DFN-CERT
  - Participant of the *eCSIRT* and *leurre.com* projects.
  - Deployment of *nepenthes* sensors to capture known malware.
  - Use of sensor networks to collect netflow information.
  - Import and integration of this data into a relational database.
    - Support for incident handling service.
    - Identification of compromised systems.
    - Database allows to find correlations between incidents.
    - Compilation of statistics showing current situation.

Introduction

- Current situation, what we **can** see:
  - Massive non-selective compromise of systems for building bot-networks.
    - Abuse of bot-networks for DDoS attacks and phishing attacks.
    - Vulnerable systems are identified by massive scanning activity (e.g. class-B networks).
  - Time interval from publication of vulnerability to exploit decreases constantly.
  - Number of zero-day exploits for unknown vulnerabilities increase constantly.
  - Web-browser and common server programs are investigated by black-hats for unknown vulnerabilities.

Introduction

- A recent incident:
  - A German university detected a compromised user system connecting to a webserver.
  - Connection to webserver has been intercepted and redirected to a honeypot.
    - URL was extracted from HTTP request.
  - Investigation of compromised user system revealed installed Goldun/Haxdoor trojan:
    - Goldun monitors use of Internet Explorer and sends captured data (URLs, content of HTML-Forms, and Passwords) to central server.
    - Attacker can download trojan data from central server.
    - Captured URL allowed to access the trojan data.

Introduction

- A recent incident:
  - Captured URL allowed to identify location of trojan Log-server
  - Trojan log-data included:
    - Ebay accounts and passwords.
    - Web-mail accounts and passwords.
    - Home-banking session data.
  - Large number of dial-in systems from german ISPs were affected.
  - Monitored users were warned in cooperation with universities, ISPs and other affected sites.

Introduction

- Current situation, what is **difficult** for us to see at the moment:
  - Selective attacks:
    - Selective attacks do not leave behind any obvious traces are in general hardly detected.
    - No obvious network activity originates from compromised hosts.
  - Early deployment of zero-day exploits:
    - How to distinguish from known exploits?
    - Early deployment of zero-day exploits is nearly invisible in background noise!

Honeynet Projects

- *Ecsirt, leurre.com*, and *Nepenthes:*
  - Deployment of widespread network of low-interaction honeypots.
    - Malware (e.g. trojans and exploit code) is automaticly captured.
      - This provides help to track down IRC based bot networks.
    - Compilation of statistics concerning abuse of known vulnerabilities can be done.

Honeynet Projects

- *Ecsirt, leurre.com*, and *Nepenthes:*
  - Advantage:
    - Identification of compromised systems:
      - IRC based Botnets
      - Known internet worms
    - Approaches are very effective concerning known vulnerabilities and non-selective attacks.
  - Disadvantage:
    - Detection of selective attacks and zero-day exploits is beyond the scope of these projects!
    - That is the aim of the NoAH project!

NoAH Project

- NoAH's benefits for CSIRTs:
  - Detection of zero-day vulnerabilities
  - Tracking down selective attacks
  - Analysis of unknown exploit code
  - Analysis of potential vulnerabilities

NoAH Project

- Detection of zero-day vulnerabilities:
  - Potential to cover a broad range of IP addresses in different networks.
    - Low-interaction components are used as relays to high-interaction honeypots.
    - Integration of CSIRTs, companies, ISPs, and home-users (*honey@home*) into the NoAH architecture.
  - Argos containment environment allows to generate accurate signatures for vulnerabilities and exploits.
    - Signatures and alerts can be distributed very quickly.

NoAH Project

- Detection of selective attacks:
- Why?
  - Attacker is prepared and motivated to attack the target.
    - Attack will be more sophisticated compared to non-selective attacks.
    - Better chance to detect zero-day exploits.
  - Selective attacks have usually higher impact for the victim.

NoAH Project

- How to attract an attacker?
  - Attractive can be services, position (IP address), DNS name, and bandwidth.
    - Webservice of honeypot can provide (faked) research results or other attractive data (Clifford Stoll's “*Cuckoo's Egg*”).
    - Honeypot is located in network of company or research institute.
    - DNS name can pretend to be an attractive target (e.g. router, server).

NoAH Project

- How to use NoAH's architecture to track down selective attacks:
  - Low-interaction components (relays) can be easily integrated into arbitrary networks.
  - High-interaction honeypots (e.g. argos) allow to provide real services (web server).
  - NoAH components can be deployed in sensitive networks with acceptable risk for the deploying site.
  - Honeypot data is analyzed at the NoAH core.
    - Deploying site do not need to spend effort into the analysis.
    - Results are distributed to the affected sites.

NoAH Project

- Analysis of unknown exploit code:
  - Some products exist for monitoring malware at execution time (e.g. norman sandbox).
  - These products do not directly support the analysis of unknown exploit code:
    - Which vulnerability is being exploited?
    - Is the vulnerability already known?
    - Is the exploit working at all?

NoAH Project

- Analysis of unknown exploit code:
  - Exploit code can be analysed and identified using argos:
    - Argos alert indicates succesfull application.
      - Exploit is detected before it gains control over the attacked machine.
      - Exploit code does not have to be fully working (e.g. due to wrong pointer offset).
    - Exploit can be identified by the corresponding argos signature.

NoAH Project

- Analysis of potential Vulnerabilities:
  - My browser crashes, is this an unknown security problem?
  - Yes, if sensitive memory structures are overwritten by user data.
  - Argos can solve this problem:
    - Deploy the browser in the argos containment environment.
    - If argos raises an alert, a security problem can be expected.

NoAH Project

- Thank you!
- Questions?