Honeynet/pot : Testing your infrastructure

like the attackers from port scanning to fuzzing

Alexandre Dulaunoy

ASBL CSRRT-LU (Computer Security Research and Response Team Luxembourg)
http://www.csrrt.org/

March 16, 2007

Testing data control ? data capture ? data collection ?

- Data Control
  - The way to contain/limit the attackers. This is the really important part to limit the potential abuse of the attackers.
  - Test : abuse the network connectivity, ...
- Data Capture
  - Capturing the activities inside and around the honeynet/pot without informing the attackers.
  - Test : overflow the data capture, generate random traffic, ...
- Data Collection
  - Collection is used to gather all the data captured in different distributed honeynets/pots.
  - Test : abusing the network protocols used, fuzzing software used, ...

Assessment of your honeynet/pot ?

- Standard approach : Vulnerability Scanning, Network Security Assessment and Penetration Testing
  - Host Enumeration (don't forget to see how your honeynet will be seen by the attackers)
- Software Analysis : Code Review to Fuzzing
- Recurring Security Assessment
  - Be aware of the data collection and the separation of collected data when doing an assessment

Testing your Honeynet/pot software with fuzzing

- Fuzzing is a simple software testing method that provides random data to the input of software
- Fuzzing is a kind of "black box" testing as the technique is looking at the behavior of the software based on the input given
- Based on the failure and the "fuzzy" input given, we could deduce the potential (often security) defect

Testing your Honeynet/pot software with fuzzing - zzuf

- zzuf is a transparent application input fuzzer.
- zzuf is intercepting file or network operation and randomly changes the input
- zzuf -s1 -r0.01 /bin/cat test-data
- zzuf is deterministic (nifty for debugging) -r0.01 is 1
- can be used to check parsing of configuration file but also network input

Q and A

- Thanks for listening.