The use of Honeynets to detect exploited systems across large enterprise networks

J. Levine, R. LaBella, H. Owen, D. Contis, and B. Culver, presented at Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, 2003.

Presented by Richard Barker

Paper Synopsis

- Discusses the deployment of a Honeynet on the Georgia Tech. Enterprise network.
- Identifies some inadequacies of existing security measures (a firewall and an Intrusion Detection System) identifying the need for a Honeynet.
- Gives an exact description of their Honeynet installation.

Shortfalls of Existing Security Mechanisms

- Firewalls don’t check:
  - Traffic which bypasses them, such as dial-up connections,
  - Traffic within the Network;
  - The transfer of files embedded with viruses is undetected; and
  - They may be overwhelmed by high volumes of traffic.
- Intrusion Detection Systems (IDS) are associated with a high level of false positives and false negatives.

Critical Comment (1)

- “[A] Honeynet can compliment (sic) the use of [a] firewall and IDS [to] help overcome these shortcomings…”
- No analysis of the Honeynet is carried out against the *identified* inadequacies of Firewalls and IDSs.
- Therefore whether Honeynets do in fact complement (complete) a security system is unproven by the paper.

Do Honeynets correct existing Security System shortfalls? (1)

- The problem, associated with firewalls, of ensuring interception of traffic is not pertinent because Honeynets detect malicious activity, which in turn leads to the traffic.
- Honeynets cannot detect the transfer of files with enclosed viruses because no analysis is carried out on traffic until it is the culprit of malevolent activity.

Do Honeynets correct existing Security System shortfalls? (2)

- The overwhelming of a Honeynet with a high-volume of traffic is:
  - unlikely because the Honeynet is by definition of no production value; and secondly
  - not applicatory because the analysis of traffic is not a run-time exercise.
- Mistaken identifications (false negatives and positives) are less probable because analysis is a human task.

Critical Comment (2)

- The article goes into excessive detail of their Honeynet system:
  - for example the CD burner software used to archive records is named; and
  - At least half of the article, for this reason, is irrelevant to the class as the article simply states facts and provides little discussion.

Appreciative Comment

- The paper gives a good background to Honeynets explaining both the need
  - The identified existing inadequacies

  And some, non-obvious, fundamental properties.
  - “A Honeynet has no production value and should [therefore] not be generating or receiving any traffic.”

Discussion

- Do Honeynets have an application outside of Enterprise Networks, for example being used in addition to a firewall on a Home Computer?