Intrusion and Intrusion Detection

Author: John McHugh

Published online: 27 July 2001

International Journal of Information Security, Volume 1 Issue 1 (2001), p 14-35

Available online by Augest, 2004:

http://www.cs.jhu.edu/~fabian/courses/CS600.424/course_papers/McHugh.pdf

Present by Zhichao Liu

Summary

- **The historical overview**
  - The evolution of attack sophistication
  - The devolution of attacker skill

--(Figure2 On Page 5)

- **Intrusion detection methods**
  - Data collection
  - Analytical approaches

Appreciative Comments

- The description of primary intrusion detection methods is easy to understand.
- Detailed examples are given to explain complex problems.
  - How the Morris Worm attacks.
  - It is hard to abstract the accurate signature from data collected by network-based sensing.
  - The threat that the audit data may be erased before being detected.

Data collection

- **Host/applications-based data collection**
  - Collect audit data from the host being monitored
  - Purpose: collect enough audit data to detect attack from the OS or applications
- **Network-based data collection**
  - Collect audit data from the network segment being observed.
  - Purpose: collect audit data to detec attack from network.
  - Advantage: a single sensor can monitor multiple hosts.
  - Disadvantage: cannot see attacks from system console, may be attacked, may be bypassed, etc.

Analytical approaches

- **Anomaly-based intrusion detection**
  - Analyse the audit data and look for anomalies.
  - Have chances to recognize novel attacks.
  - Difficult to classify or name attacks.
    - What is NORMAL?
- **Signature-based detection**
  - Detect attacks by checking if the sensed data matches a specific attack description.
  - Hard to figure out the signature of an attack.
  - If well defined, the detection will be easy and accurate.
  - Weak in identify novel attacks.

Criticism

- **Unorganized classification may cause misunderstand about IDS.**
  - **Two more categories: passive system and reactive system.**(http://www.webopedia.com/TERM/I/intrusion_detection_system.html)
  - **Three different taxonomies.**
    - **Data collection methods**
    - **Analytical approaches**
    - **Different kind of reactions**
  - **Example: ISS(Internet Security Systems)**
    - **Data collection methods: both.**
    - **Analytical approaches: not mentioned**
    - **Reactions: not mentioned**

Question

- **Why we need Network-based data collection?**
  - **Commercial?**
    - **Still need local protection on every single host.**
  - **Easy to construct?**
    - **How about it is not necessary.**
  - **Safety?**
    - **The sensor itself might be attacked or bypassed.**
  - **Or any thing else?**
    - **Difficult to implement all in one?**
    - **Make business? More jobs for us?**