Chapter 8
Intrusion Detection

Definitions

• Intrusion
  – A set of actions aimed to compromise the security goals, namely
    • Integrity, confidentiality, or availability, of a computing and networking resource
• Intrusion detection
  – The process of identifying and responding to intrusion activities
• Intrusion prevention
  – Extension of ID with exercises of access control to protect computers from exploitation
• IDP - Intrusion Detection & Prevention
IDP Analogy: Protecting Your Home

- **Prevention**
  - Locked doors, secured windows, wall around property etc.
- **Detection**
  - Motion detectors, fire alarm, dog
- **We need both**
- **We may also need a response**
  - Call police, disable intruders etc.

Intrusion Techniques

- **Objective is to gain access or increase privileges**
- **Initial attacks often exploit system or software vulnerabilities**
  - To execute code to get backdoor
    - e.g. buffer overflow
  - Or to gain protected information
    - e.g. password guessing or acquisition
- **Further attacks try to escalate privileges**

Elements of Intrusion Detection System

- **Audit Data**
  - Audit Records
- **Activity Data**
  - Detection Engine
  - Alarms
- **Decision Table**
  - Action/Report
Intrusion Detection Systems

• Modeling
  – Features: evidences extracted from audit data
  – Analysis approach: piecing the evidences together
    • Misuse detection (a.k.a. signature-based)
    • Anomaly detection (a.k.a. statistical-based)

• Deployment: Network-based or Host-based
  – Network based: monitor network traffic
  – Host based: monitor computer processes

Intrusion Detection Systems

• Logical components:
  – Sensors - collect data
  – Analyzers - determine if intrusion has occurred
  – User interface - manage / direct / view IDS

IDS Principles

• Assume intruder behavior differs from legitimate users
  – Expect overlap as shown
  – Observe deviations from past history
  – Problems of:
    • False positives
    • False negatives
    • Need to compromise
Misuse / Signature Detection

Example: if (src_ip == dst_ip) then “land attack”

Signature Detection

• Observe events on system and apply a set of rules to decide if intruder

• Approaches:
  - Rule-based anomaly detection
    • Analyze historical audit records for expected behavior, then match with current behavior
  - Rule-based penetration identification
    • Rules identify known penetrations / weaknesses
    • Often by analyzing attack scripts from Internet
    • Supplemented with rules from security experts

Example Illegal Privileged Account Access Rule

```
(defrule illegal_privileged_account_example
  if there exists a failed_login_event
    such that name is ("root" or "superuser" or "maintenance" or "system") and
    time is "time_stamp" and
    channel is "channel"
  then
    (print "WARNING: ATTEMPTED LOGIN TO PRIVILEGED ACCOUNT")
    and remember a breakin_attempt
    with certainty "high"
    such that attack_time is "time_stamp"
    and login_channel is "channel"
```
Discussion

• Advantages:
  – Simple Design
  – Fast
  – Can be designed to handle various types of audit information

• Disadvantages
  – Cannot detect new attacks / zero day attacks

Anomaly Detection

• Threshold detection
  – Checks excessive event occurrences over time
    • Alone a crude and ineffective intruder detector
    • Must determine both thresholds and time intervals

• Profile based
  – Characterize past behavior of users / groups
  – Then detect significant deviations
  – Based on analysis of audit records
    • Gather metrics: counter, gauge, interval timer, resource utilization
    • Analyze: mean and standard deviation, multivariate, Markov process, time series, operational model
### Example of User Profile

**Table 1: Example data.** The table entries represent the percentage a legitimate user employed a given command, based on groupings of 1,000 commands per user.

<table>
<thead>
<tr>
<th></th>
<th>comp</th>
<th>exit</th>
<th>login</th>
<th>suid</th>
<th>rsh</th>
<th>kill</th>
</tr>
</thead>
<tbody>
<tr>
<td>w0</td>
<td>1.2%</td>
<td>1.1%</td>
<td>1.5%</td>
<td>1.5%</td>
<td>1.5%</td>
<td>1.5%</td>
</tr>
<tr>
<td>w1</td>
<td>2.5%</td>
<td>1.1%</td>
<td>1.5%</td>
<td>1.5%</td>
<td>1.5%</td>
<td>1.5%</td>
</tr>
<tr>
<td>w2</td>
<td>3.6%</td>
<td>1.1%</td>
<td>1.5%</td>
<td>1.5%</td>
<td>1.5%</td>
<td>1.5%</td>
</tr>
<tr>
<td>w3</td>
<td>4.0%</td>
<td>1.1%</td>
<td>1.5%</td>
<td>1.5%</td>
<td>1.5%</td>
<td>1.5%</td>
</tr>
</tbody>
</table>

Source: J. Marin et al. “A Hybrid Approach to the Profile Creation and Intrusion Detection”

### Discussion

- **Advantages**
  - Has the potential to detect new attacks / zero day attacks

- **Disadvantages**
  - Depends on quality of data used to define normal behavior
  - High false positive rates
    - Anomalies can just be new normal activities.
    - Anomalies caused by other element faults such as router failure or misconfiguration

- Need to be re-trained periodically

### Host-Based IDS

- **Specialized software to monitor system activity to detect suspicious behavior**
  - Primary purpose is to detect intrusions, log suspicious events, and send alerts
  - Can detect both external and internal intrusions

- **Using OS auditing mechanism**
  - E.g. BSM on Solaris: logs all direct and indirect events generated by a user
  - *strace* for system calls made by a program

- **Monitoring user activities**
  - E.g. analyze shell commands
Audit Records

- A fundamental tool for host-based intrusion detection
- Two variants:
  - Native audit records - provided by O/S
    - Always available
    - May not contain needed information
    - Needed information may not be in convenient form
  - Detection-specific audit records - IDS specific
    - Additional overhead but specific to IDS task
    - Often log individual elementary actions
    - e.g. may contain fields for: subject, action, object, exception-condition, resource-usage, time-stamp

Distributed Host-Based IDS

- Deploying sensors at strategic locations
  - E.G., Packet sniffing via tcpdump at routers
- Inspecting network traffic
  - Watch for violations of protocols and unusual connection patterns
- Monitoring user activities
  - Look into the data portions of the packets for malicious code
- May be easily defeated by encryption
  - Data portions and some header information can be encrypted
  - Nonetheless, the decryption engine may still be there, especially for exploit

Network IDSs
Honeypots

- Are decoy systems
  - Filled with fabricated info
  - Instrumented with monitors / event loggers
  - Divert and hold attacker to collect activity info
  - Without exposing production systems
- Initially were single systems
- More recently are entire network / emulate entire networks (Honeynets)
Honeypot Deployment

Summary

• Introduced intruders & intrusion detection
  – Hackers, criminals, insiders
• Intrusion detection approaches
  – Host-based (single and distributed)
  – Network
  – Distributed adaptive
  – Exchange format
• Honey pots