Intrusion Detection

Daniel Bosk

Department of Information and Communication Systems (ICS),
Mid Sweden University, Sundsvall.

intrusion.tex 1493 2013-12-02 11:34:40Z danbos

Översikt

1. Intruders
   - Intruders
   - Behaviour Patterns
   - Intrusion Techniques
2. Intrusion Detection
   - Intrusion Detection
   - Audit Records
   - Statistical Anomaly Detection
   - Rule-Based Intrusion Detection
   - Distributed Intrusion Detection
   - Honeypots
3. Password Management
   - Bloom Filter

Litteratur

The lecture gives an overview of chapter 11 “Intruders” in [Sta13] and chapter 21 “Network Attack and Defense” in [And08].
When you have reviewed the material you should solve problems 11.2, 11.3, 11.4, 11.6, and 11.9 in [Sta13].

Översikt

1. Intruders
   - Intruders
   - Behaviour Patterns
   - Intrusion Techniques
2. Intrusion Detection
   - Intrusion Detection
   - Audit Records
   - Statistical Anomaly Detection
   - Rule-Based Intrusion Detection
   - Distributed Intrusion Detection
   - Honeypots
3. Password Management
   - Bloom Filter

Intruders

Masquerader A user who is not authorized to use the system who penetrates the access control of the system to exploit the user account of a legitimate user. Typically outsider.

Misfeasor A legitimate user who accesses resources for which such access is not authorized, or who misuses his or her privileges. Typically insider.

Clandestine user An individual who seizes supervisory control of the system and uses this control to evade auditing or to supress audit collection. Can be either insider or outsider.

Behaviour Patterns

- The behaviour will typically be different from that of ordinary users.
- The “hacker” will look for targets of opportunities. Exploratory in nature. Target design for IDSs.
- The criminal organisations will target specific systems of interest. They will try to obscure the usage patterns. These usually make a quick hit, once in they gather as much information as possible and then leave. Think APT. A little harder for IDSs to detect due to quick nature.
- The insider will just take information available to him or her. No access control is usually breached. Counter by principle of least privilege, logs, strong authentication, terminate employees’ accounts.

Intrusion Techniques

1. Try default passwords with standard accounts.
2. Exhaustively try all short passwords.
3. Try a dictionary attack.
4. Collect information about the system users; e.g. full names, names of spouses and children, pictures in their offices.
5. Try users' phone numbers, personal ID number, room numbers.
6. Try license plate numbers.
7. Use a Trojan horse to bypass restrictions on access.
8. Tap the connection between a remote user and the host system.

Översikt

1. Intruders
   - Intruders
   - Behaviour Patterns
   - Intrusion Techniques
2. Intrusion Detection
   - Intrusion Detection
   - Audit Records
   - Statistical Anomaly Detection
   - Rule-Based Intrusion Detection
   - Distributed Intrusion Detection
   - Honeypots
3. Password Management
   - Bloom Filter

Mittuniversitetet
MID SWEDEN UNIVERSITY

Intrusion Detection

- Intrusion detection is a difficult task.
- Based on the assumption that behaviour of intruder and legitimate user can be quantified, and hence differences found.
- Problem is these behaviours might sometimes overlap.

Intrusion Detection

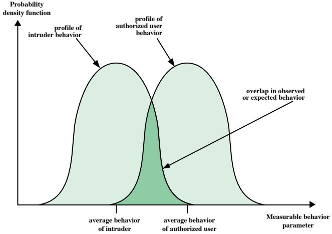

Figure 11.1 Profiles of Behavior of Intruders and Authorized Users

Figure : User behavioural profiles. Image: [Sta13].

Intrusion Detection

- False positives: authorised users detected as intruders.
- False negatives: intruders detected as legitimate users.
- We can reasonably well distinguish masqueraders through past history.
- Misfeasors can be detected by defining what's unauthorised use.
- Clandestine user is very difficult to detect automatically.

Audit Records

- Native audit records: log all (relevant) user activity using system logs.
- Detection-specific audit records: filters out events interesting for the IDS.
- Example: copying a file.

Statistical Anomaly Detection

- Threshold detection: defining thresholds independent of users.
- Profile based: use a profile for each user to detect changes in behaviour.

Rule-Based Intrusion Detection

- Rule-based detection: defines rules for attack patterns, also called signature detection.

Distributed Intrusion Detection

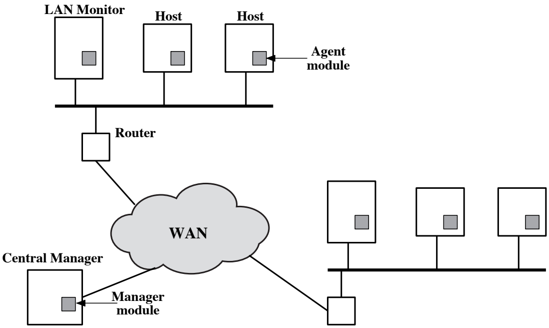

Figure 11.2 Architecture for Distributed Intrusion Detection

Figure : Distributed Intrusion Detection System. Image: [Sta13].

Honeypots

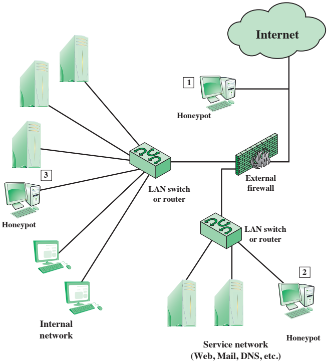

Figure 11.4 Example of Honeypot Deployment

Figure : An illustration of honeypots. Image: [Sta13].

Översikt

1. Intruders
   - Intruders
   - Behaviour Patterns
   - Intrusion Techniques
2. Intrusion Detection
   - Intrusion Detection
   - Audit Records
   - Statistical Anomaly Detection
   - Rule-Based Intrusion Detection
   - Distributed Intrusion Detection
   - Honeypots
3. Password Management
   - Bloom Filter

Mittuniversitetet
MID SWEDEN UNIVERSITY

Bloom Filter

Referenser I

Ross J. Anderson. *Security engineering : a guide to building dependable distributed systems*. 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: `http://www.cl.cam.ac.uk/~rja14/book.html`.

William Stallings. *Network security essentials : applications and standards*. 5th ed. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.

Mittuniversitetet
MID SWEDEN UNIVERSITY