0790326
Intrusion Detection and Prevention Systems

2023/2024 – Semester 2

Week 10

28tH April 2024

جامعة فيلادلفيا
Philadelphia University

Dr. Basil Elmasri
balmasri@philadelphia.edu.jo

External Material

- Rest of the slides for this week are based on (Stallings & Brown, 2024) book, chapter 8.
  - Some extra slides have been added, their text was taken from the book.
  - Footers, dates, and slides number have been added only to help students reading the material.
- Study and exams will be based on the book chapters, not the slides.

Data Sources and Sensors (I)

- A fundamental component of intrusion detection is the sensor that collects data
- Common data sources include:
  - System call traces
  - Audit (log file) records
  - File integrity checksums
  - Registry access

Data Sources and Sensors (II)

- **System call traces**: A record of the sequence of systems calls by processes on a system is the preferred data source.
- Work well on Unix and Linux systems, they are problematic on Windows systems due to the extensive use of DLLs that obscure which processes use specific system calls.

Data Sources and Sensors (III)

- **Audit (log file) records**: most modern operating systems include accounting software that collects information on user activity.
- The advantage of using this information is that no additional collection software is needed.
- The disadvantages are that the audit records may not contain the needed information or may not contain it in a convenient form, and intruders may attempt to manipulate these records to hide their actions.

Data Sources and Sensors (IV)

- **File integrity checksums**: periodically scan critical files for changes from the desired baseline by comparing current cryptographic checksums for these files with a record of known good values.
- Disadvantages include the need to generate and protect the checksums using known good files and the difficulty of monitoring changing files.
- Tripwire is a well-known system using this approach.

Data Sources and Sensors (V)

- **Registry access**: An approach used on Windows systems is to monitor access to the registry, given the amount of information used by programs on these systems.
- However, this source is very Windows specific and has recorded limited success.

Anomaly-Based HIDSs (1 of 2)

- UNIX and Linux systems: System calls
  - Means by which programs access core kernel functions
  - Provide detailed information on process activity that can be used to classify it as normal or anomalous
  - Typically gathered using an OS hook and analyzed by a suitable decision engine
- Windows systems
  - Traditionally not used anomaly-based HIDSs
  - Used audit log entries or registry file updates as a data source
  - Neither approach was successful
- Disadvantages of system calls:
  - Impose load on the monitored system to gather and classify data
  - The training phase may require time and computational resources

Anomaly-Based HIDSs (2 of 2)

- Disadvantages of audit (log) records:
  - Have a lower detection rate than the system call trace approaches
  - More susceptible to intruder manipulation
- Looking for changes to important files on the monitored host
  - Uses a cryptographic checksum to check for changes from the known good baseline for the monitored files
  - Most widely used implementation is the tripwire system
  - Very sensitive to changes in the monitored files
  - Disadvantages
    - Cannot detect changes made to processes once they are running
    - Other difficulties are determining which files to monitor, having access to a known good copy of monitored file to establish the baseline value, and protecting the database of file signatures.

References

Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice (5 ed.). Pearson. Retrieved from https://www.pearson.com/en-us/subject-catalog/p/computer-security-principles-and-practice/P200000010333/9780138091712