Intrusion Detection

Vítor Francisco Fonte
vff@di.uminho.ot

João Marco Silva
joaomarco@di.uminho.ot

University of Minho
2019/20

Concepts

Intrusion:

- attempt to compromise confidentiality, integrity, or availability (CIA)
- attempt to bypass the security mechanisms of a computer network

Intrusion Detection System (IDS):

- process of monitoring events occurring in a computer system or network, and analysing them for signs of intrusions

Intrusion Prevention Systems (IPS):

- IDS capabilities plus mechanisms aiming to stop possible incidents

Types of Attacks: Well-Known Intrusions

- Static and well defined pattern
- Usually simple to execute
- Very little inherent variability
- Ex.: pattern match in audit records or log events

Types of Attacks: Generalised Intrusions

- Similar to well known intrusions
- But have a larger or smaller degree of variability
- Exploit more general flaws in the attacked system
- Ex.: users abusing their privileges

Types of Attacks: Unknown Intrusions

- Very general in nature
- IDS does not really know what to expect
- Ex.: masqueraded traffic behaviour

Detection Methods: Signature-Based Detection

- Knowledge-based
- Signature is a pattern or string corresponding to a known attack or threat
- Compares patterns against captured events for recognising possible intrusions

Detection Methods: Signature-Based Detection

Advantages:

- Simplest and effective method to detect known attacks

Disadvantages:

- Ineffective to detect unknown attacks and variants of known attacks
- Hard to keep signatures/patterns up to date

Detection Methods: Anomaly-Based Detection

- Behaviour-based

- Anomaly is a deviation to a known behaviour

- It takes the attitude that something that is abnormal is probably suspicious

- Ex.: failed login attempts, processor usage, network connections, Denial-of-Service (DoS)

Detection Methods: Anomaly-Based Detection

Advantages:

- Effective to detect new and unforeseen vulnerabilities
- Less dependent on OS
- Facilitate detection of privilege abuse

Disadvantages:

- Sometimes complex in defining normal and abnormal behaviour
- Difficult to trigger alerts in right time
- Weak accuracy due to observed events being constantly changed

Detection Methods: Stateful Protocol Analysis

- Specification-based
- Trace of protocol state
- Ex.: Pairing requests with replies
- Based on protocol standards

Detection Methods: Stateful Protocol Analysis

Advantages:

- Know and trace the protocol state
- Distinguish unexpected sequences of commands

Disadvantages:

- Resource consuming to protocol state tracing and examination
- Unable to inspect attacks looking like benign protocol behaviours
- Might be incompatible with proprietary protocols

Detection Approaches

Statistics-based:

- Predefined thresholds
- Mean and standard deviation

Ruled-based:

- If-Then or If-Then-Else rules are applied to construct the model and profile of well known intrusions

Pattern-based:

- Focused on known attacks through string matching
- Suitable for signature-based detection

Detection Approaches

State-based:

- Exploit finite state machine derived from network behaviours to identify attacks
- Suitable for anomaly-based and stateful protocol analysis

Heuristic-based:

- Inspired by biological concepts and artificial intelligence
- Ex.: Immune system responses

Technology Types

- Host-based IDS (HIDS)
- Network-based IDS (NIDS)
- Wireless-based IDS (WIDS)
- Network Behaviour Analysis (NBA)
- Mixed IDS (MIDS)

Effectiveness

Detection rate:

- Degree of correct intrusion classification
- Avoiding false alarms

False Positive (FP)

- When IDS incorrectly identifies benign activity as malign

False Negatives (FN)

- When IDS fails to identify malicious activity

Snort

- Very popular IDS
- Rule-based approach (4000+ rules)
- Aho-Corasick algorithm for exact signature matching
- Install and configure Snort from
  - https://www.snort.org/downloads
- Exercise:
  - Download the trace, analyze and discuss the intrusion identification
  - https://bit.ly/2PnRtaV